FlexPod 익스프레스

FlexPod

NetApp

October 30, 2025

목차

FlexPod 익스프레스 . . . 1
FlexPod Express with Cisco UCS C-Series 및 NetApp AFF C190 Series 설계 가이드 를 참조하십시오 . . . 1
NVA-1139-design:FlexPod Express with Cisco UCS C-Series 및 NetApp AFF C190 Series . . . 1
프로그램 요약 . . . 1
기술 요구 사항 . . . 2
디자인 선택 . . . 3
결론 . . . 7
추가 정보를 찾을 수 있는 위치 . . . 7
FlexPod Express with Cisco UCS C-Series 및 NetApp AFF C190 Series 구축 가이드 를 참조하십시오 . . . 8
NVA-1142-deploy: FlexPod Express with Cisco UCS C-Series 및 NetApp AFF C190 Series-NVA Deployment . . . 8
솔루션 개요 . . . 8
기술 요구 사항 . . . 11
FlexPod Express 케이블링 정보 . . . 12
구현 절차 . . . 15
결론 . . . 101
감사의 말 . . . 101
추가 정보를 찾을 수 있는 위치 . . . 102
버전 기록 . . . 102
FlexPod Express with Cisco UCS C-Series and AFF A220 Series 설계 가이드 를 참조하십시오 . . . 102
NVA-1125-design: FlexPod Express with Cisco UCS C-Series and AFF A220 Series . . . 102
프로그램 요약 . . . 102
솔루션 개요 . . . 104
기술 요구 사항 . . . 105
디자인 선택 . . . 106
솔루션 검증 . . . 111
결론 . . . 112
추가 정보를 찾을 수 있는 위치 . . . 112
FlexPod Express with Cisco UCS C-Series and AFF A220 Series 구축 가이드 를 참조하십시오 . . . 112
NVA-1123-deploy:FlexPod Express with VMware vSphere 6.7 and NetApp AFF A220 구축 가이드 . . . 112
솔루션 개요 . . . 113
기술 요구 사항 . . . 115
FlexPod Express 케이블링 정보 . . . 116
구현 절차 . . . 119
결론 . . . 193
추가 정보를 찾을 수 있는 위치 . . . 193
직접 연결 IP 기반 스토리지를 사용하는 VMware vSphere 6.7U1 및 NetApp AFF A220을 지원하는 FlexPod Express . . . 193
NVA-1131-deploy: VMware vSphere 6.7U1 및 NetApp AFF A220을 지원하는 FlexPod Express(직접

연결 IP 기반 스토리지 포함 193
솔루션 개요 194
기술 요구 사항 197
FlexPod 익스프레스 케이블 연결 정보 197
구현 절차 199
결론 303
추가 정보 304
FlexPod Express for VMware vSphere 7.0 with Cisco UCS Mini 및 NetApp AFF/FAS-NVA-Deployment 304

FlexPod 익스프레스

FlexPod Express with Cisco UCS C-Series 및 NetApp AFF C190 Series 설계 가이드 를 참조하십시오

NVA-1139-design:FlexPod Express with Cisco UCS C-Series 및 NetApp AFF C190 Series

Savita Kumari, NetApp에서 기술 지원

파트너 후원:[오류: 그래픽 이미지가 없습니다]

업계 동향에 따르면 많은 데이터 센터가 공유 인프라 및 클라우드 컴퓨팅으로 전환하고 있습니다. 또한 기업에서는 데이터 센터에서 친숙한 기술을 사용하는 원격 사무소 및 지사를 위해 간편하고 효율적인 솔루션을 찾고 있습니다.

FlexPod Express는 Cisco UCS(Cisco Unified Computing System), Cisco Nexus 스위치 제품군, NetApp AFF 시스템을 기반으로 사전 설계되고 모범 사례 데이터 센터 아키텍처입니다. FlexPod Express의 구성 요소는 FlexPod 데이터 센터 구성 요소와 비슷하므로 더 작은 규모로 전체 IT 인프라 환경에서 관리 시너지 효과를 실현할 수 있습니다. FlexPod 데이터 센터 및 FlexPod 익스프레스는 가상화 및 베어 메탈 운영 체제 및 엔터프라이즈 워크로드를 위한 최적의 플랫폼입니다.

"다음: 프로그램 요약."

프로그램 요약

FlexPod 통합 인프라 포트폴리오

FlexPod 참조 아키텍처는 CVD(Cisco Validated Design) 또는 NVA(NetApp Verified Architecture)로 제공됩니다. 특정 CVD 또는 NVA의 고객 요구 사항을 기반으로 한 편차는 이러한 변형으로 인해 지원되지 않는 구성이 구축되지 않는 경우 허용됩니다.

다음 그림과 같이 FlexPod 포트폴리오에는 FlexPod 익스프레스 및 FlexPod 데이터 센터 솔루션이 포함되어 있습니다.

- * FlexPod 익스프레스 * 는 Cisco 및 NetApp의 기술을 사용하는 엔트리 레벨 솔루션입니다.
- * FlexPod 데이터 센터 * 는 다양한 워크로드 및 애플리케이션을 위한 최적의 다목적 토대를 제공합니다.

[오류: 그래픽 이미지가 없습니다]

NetApp 검증 아키텍처 프로그램

NetApp 검증 아키텍처 프로그램에서는 NetApp 솔루션을 위한 검증된 아키텍처를 고객에게 제공합니다. NVA 솔루션의 특징은 다음과 같습니다.

- 철저한 테스트를 거친 아키텍처
- 기본적으로 규범적인 아키텍처
- 구축 위험 최소화

- 출시 시간 단축 이 가이드는 VMware vSphere를 사용한 FlexPod Express 설계에 대해 자세히 설명합니다.

또한, 이 설계에서는 NetApp ONTAP 9.6 소프트웨어, Cisco Nexus 31108 스위치 및 Cisco UCS C220 M5 서버를 하이퍼바이저 노드로 실행하는 완전히 새로운 AFF C190 시스템을 활용합니다.

솔루션 개요

FlexPod Express는 혼합 가상화 워크로드를 실행하도록 설계되었습니다. 원격 사무소, 지점 및 중소 및 중견 기업을 타겟으로 합니다. 또한 특정 목적에 맞는 전용 솔루션을 구현하려는 대규모 기업에도 적합합니다. FlexPod 익스프레스를 위한 이 새로운 솔루션은 NetApp ONTAP 9.6, NetApp AFF C190 시스템 및 VMware vSphere 6.7U2와 같은 새로운 기술을 추가합니다.

다음 그림에서는 FlexPod Express 솔루션에 포함된 하드웨어 구성 요소를 보여 줍니다.

[오류: 그래픽 이미지가 없습니다]

대상

이 문서는 IT 효율성을 제공하고 IT 혁신을 지원하기 위해 구축된 인프라를 활용하려는 사용자를 위해 작성되었습니다. 이 문서의 대상에는 세일즈 엔지니어, 현장 컨설턴트, 프로페셔널 서비스 직원, IT 매니저, 파트너 엔지니어 및 고객.

솔루션 기술

이 솔루션은 NetApp, Cisco 및 VMware의 최신 기술을 활용합니다. 이 제품은 ONTAP 9.6 소프트웨어, 이중 Cisco Nexus 31108 스위치 및 VMware vSphere 6.7U2를 실행하는 Cisco UCS C220 M5 랙 서버를 실행하는 새로운 NetApp AFF C190 시스템을 갖추고 있습니다. 다음 그림에 나와 있는 검증된 이 솔루션은 10기가비트 이더넷(10GbE) 기술을 사용합니다. 또한 FlexPod 익스프레스 아키텍처가 조직의 변화하는 비즈니스 요구에 적응할 수 있도록 한 번에 두 개의 하이퍼바이저 노드를 추가하여 확장하는 방법에 대한 지침도 제공됩니다.

[오류: 그래픽 이미지가 없습니다]

"다음: 기술 요구 사항."

기술 요구 사항

FlexPod Express를 사용하려면 선택한 하이퍼바이저와 네트워크 속도에 따라 하드웨어 및 소프트웨어 구성요소를 조합해야 합니다. 또한 FlexPod Express는 하이퍼바이저 노드를 시스템에 추가하는 데 필요한 하드웨어 구성요소를 2개 단위로 배치합니다.

하드웨어 요구 사항

선택한 하이퍼바이저에 관계없이 모든 FlexPod Express 구성은 동일한 하드웨어를 사용합니다. 따라서 비즈니스 요구사항이 변경되더라도 동일한 FlexPod Express 하드웨어에서 다른 하이퍼바이저를 사용할 수 있습니다.

다음 표에는 이 FlexPod Express 구성과 이 솔루션 구축에 필요한 하드웨어 구성요소가 나와 있습니다. 솔루션 구현에 사용되는 하드웨어 구성요소는 고객 요구사항에 따라 다를 수 있습니다.

하드웨어	수량
AFF C190 2노드 클러스터	1
Cisco UCS C220 M5 서버	2

하드웨어	수량
Cisco Nexus 31108 스위치	2
Cisco UCS C220 M5 랙 서버용 Cisco UCS VIC(Virtual Interface Card) 1457	2

소프트웨어 요구 사항

다음 표에는 FlexPod 익스프레스 솔루션의 아키텍처를 구현하는 데 필요한 소프트웨어 구성 요소가 나열되어 있습니다.

소프트웨어	버전	세부 정보
CIMC(Cisco Integrated Management Controller)	4.0.4	C220 M5 랙 서버용
Cisco NX-OS입니다	7.0(3) i7(6)	Cisco Nexus 31108 스위치의 경우
NetApp ONTAP를 참조하십시오	9.6	NetApp AFF C190 컨트롤러의 경우

다음 표에는 FlexPod Express의 모든 VMware vSphere 구축에 필요한 소프트웨어가 나와 있습니다.

소프트웨어	버전
VMware vCenter Server 어플라이언스	6.7U2
VMware vSphere ESXi	6.7U2
ESXi용 NetApp VAAI 플러그인	1.1.2
NetApp 가상 스토리지 콘솔	9.6

"다음: 디자인 선택."

디자인 선택

이 섹션에 나열된 기술은 아키텍처 설계 단계에서 선택되었습니다. 각 기술은 FlexPod 익스프레스 인프라 솔루션에서 특정 목적에 부합합니다.

ONTAP 9.6이 설치된 **NetApp AFF C190** 시리즈

이 솔루션은 NetApp AFF C190 시스템 및 ONTAP 9.6 소프트웨어의 최신 NetApp 제품 중 2개를 활용합니다.

AFF C190 시스템

대상 그룹은 경제적인 가격으로 All-Flash 기술로 IT 인프라를 현대화하려는 고객입니다. AFF C190 시스템은 새로운 ONTAP 9.6 및 플래시 번들 라이센스와 함께 제공됩니다. 즉, 다음 기능이 탑재되어 있습니다.

- CIFS, NFS, iSCSI 및 FCP
- NetApp SnapMirror 데이터 복제 소프트웨어, NetApp SnapVault 백업 소프트웨어, NetApp SnapRestore 데이터 복구 소프트웨어, NetApp SnapManager 스토리지 관리 소프트웨어 제품군 및 NetApp SnapCenter 소프트웨어
- FlexVol 기술
- 중복제거, 압축, 컴팩션

- 씬 프로비저닝
- 스토리지 QoS
- NetApp RAID DP 기술
- NetApp Snapshot 기술
- FabricPool

다음 그림은 호스트 접속에 대한 두 가지 옵션을 보여 줍니다.

다음 그림에서는 SFP+ 모듈을 삽입할 수 있는 UTA 2 포트를 보여 줍니다.

[오류: 그래픽 이미지가 없습니다]

다음 그림은 기존 RJ-45 이더넷 케이블을 통한 연결을 위한 10GBASE-T 포트를 보여줍니다.

[오류: 그래픽 이미지가 없습니다]

10GBASE-T 포트 옵션의 경우 10GBASE-T 기반 업링크 스위치가 있어야 합니다.

AFF C190 시스템은 960GB SSD에서만 제공됩니다. 다음 네 가지 확장 단계를 선택할 수 있습니다.

- 8x 960GB
- 12x 960GB
- 18x 960GB
- 24x 960GB

AFF C190 하드웨어 시스템에 대한 자세한 내용은 를 참조하십시오 "NetApp AFF C190 All-Flash 어레이 페이지".

ONTAP 9.6 소프트웨어

NetApp AFF C190 시스템은 새로운 ONTAP 9.6 데이터 관리 소프트웨어를 사용합니다. ONTAP 9.6은 업계 최고의 엔터프라이즈 데이터 관리 소프트웨어입니다. 새로운 버전에는 새로운 수준의 단순성과 유연성, 강력한 데이터 관리 기능, 스토리지 효율성, 업계 최고 수준의 클라우드 통합이 결합되어 있습니다.

ONTAP 9.6에는 FlexPod 익스프레스 솔루션에 적합한 여러 가지 기능이 있습니다. 가장 중요한 것은 NetApp이 스토리지 효율성을 위해 노력하고 있다는 점입니다. 이는 소규모 구축에 있어서 가장 중요한 기능 중 하나입니다. 중복제거, 압축, 컴팩션, 씬 프로비저닝 같은 NetApp 스토리지 효율성 기능의 특징은 ONTAP 9.6에서 확인할 수 있습니다. NetApp WAFL 시스템은 항상 4KB 블록을 씁니다. 블록이 4KB의 할당된 공간을 사용하지 않을 때 다중 블록을 4KB 블록으로 결합합니다. 다음 그림에서는 이 프로세스를 보여 줍니다.

[오류: 그래픽 이미지가 없습니다]

ONTAP 9.6은 이제 NVMe 볼륨의 선택적 512바이트 블록 크기를 지원합니다. 이 기능은 기본적으로 512바이트 블록을 사용하는 VMware VMFS(Virtual Machine File System)에서 원활하게 작동합니다. 기본 4K 크기를 그대로 사용하거나 512바이트 블록 크기를 선택적으로 설정할 수 있습니다.

ONTAP 9.6의 기타 향상된 기능은 다음과 같습니다.

- * NetApp Aggregate Encryption(NAE). * NAE는 애그리게이트 레벨에서 키를 할당하며, 따라서 애그리게이트의 모든 볼륨을 암호화합니다. 이 기능을 사용하면 볼륨을 애그리게이트 레벨에서 암호화 및 중복제거할 수 있습니다.

- NetApp ONTAP FlexGroup 볼륨 개선 *. ONTAP 9.6에서는 FlexGroup 볼륨의 이름을 쉽게 변경할 수 있습니다. 데이터를 로 마이그레이션하기 위해 새 볼륨을 생성할 필요가 없습니다. ONTAP 시스템 관리자 또는 CLI를 사용하여 볼륨 크기를 줄일 수도 있습니다.
- * FabricPool 개선. * ONTAP 9.6은 오브젝트 저장소를 클라우드 계층으로 추가로 지원합니다. 또한 Google Cloud 및 Alibaba Cloud Object Storage Service(OSS)에 대한 지원도 목록에 추가되었습니다. FabricPool은 AWS S3, Azure Blob, IBM Cloud 오브젝트 스토리지 및 NetApp StorageGRID 오브젝트 기반 스토리지 소프트웨어를 비롯한 여러 오브젝트 저장소를 지원합니다.
- SnapMirror 향상 기능 * ONTAP 9.6에서는 소스 어레이를 떠나기 전에 새 볼륨 복제 관계가 기본적으로 암호화되고 SnapMirror 대상에서 암호가 해독됩니다.

Cisco Nexus 3000 시리즈

Cisco Nexus 31108PC-V는 48개의 SFP+ 포트와 6개의 QSFP28 포트를 갖춘 10Gbps SFP+ 기반 ToR(Top-of-Rack) 스위치입니다. 각 SFP+ 포트는 100Mbps, 10Gbps 속도에서 작동할 수 있으며, 각 QSFP28 포트는 네이티브 100Gbps 또는 40Gbps 모드 또는 4x 10Gbps 모드로 작동할 수 있어 유연한 마이그레이션 옵션을 제공합니다. 이 스위치는 짧은 지연 시간과 낮은 전력 소비에 최적화된 진정한 PHY 없는 스위치입니다.

Cisco Nexus 31108PC-V 사양에는 다음 구성 요소가 포함됩니다.

- 31108PC-V에서 최대 1.2Tbps의 스위칭 용량 및 포워딩 속도 2.16Tbps
- 48개의 SFP 포트는 1 및 10기가비트 이더넷(10GbE)을 지원하며, 6개의 QSFP28 포트는 각각 4개의 10GbE 또는 40GbE 또는 100GbE를 지원합니다

다음 그림은 Cisco Nexus 31108PC-V 스위치입니다.

[오류: 그래픽 이미지가 없습니다]

Cisco Nexus 31108PC-V 스위치에 대한 자세한 내용은 을 참조하십시오 "Cisco Nexus 3172PQ, 3172TQ, 3172TQ-32T, 3172PQ-XL 및 3172TQ-XL 스위치 데이터 시트".

Cisco UCS C-Series 를 참조하십시오

FlexPod 익스프레스 구축에서는 다양한 구성 옵션으로 Cisco UCS C-Series 랙 서버를 FlexPod 익스프레스 설치시 특정 요구사항에 맞게 구성할 수 있기 때문에 Cisco UCS C-Series 랙 서버를 선택했습니다.

Cisco UCS C-Series 랙 서버는 업계 표준 폼 팩터에서 유니파이드 컴퓨팅을 제공하여 TCO를 절감하고 민첩성을 향상합니다.

Cisco UCS C-Series 랙 서버는 다음과 같은 이점을 제공합니다.

- Cisco UCS의 폼 팩터 중립적인 엔트리 레벨
- 애플리케이션을 간편하고 신속하게 구축
- 통합 컴퓨팅 혁신 및 이점을 랙 서버로 확장
- 친숙한 랙 패키지의 고유한 이점을 통해 고객의 선택 옵션 증가

[오류: 그래픽 이미지가 없습니다]

위 그림에 표시된 Cisco UCS C220 M5 랙 서버는 업계에서 가장 다양한 범용 엔터프라이즈 인프라 및 애플리케이션 서버 중 하나입니다. 이 서버는 가상화, 협업 및 베어 메탈 애플리케이션을 비롯하여 광범위한 워크로드에 업계 최고의 성능과 효율성을 제공하는 고밀도 2소켓 랙 서버입니다. Cisco UCS C-Series 랙 서버는 독립형 서버로 또는 Cisco

UCS의 일부로 구축할 수 있으므로 Cisco의 표준 기반 통합 컴퓨팅 혁신 기술을 활용하여 고객의 TCO를 절감하고 비즈니스 민첩성을 높일 수 있습니다.

C220 M5 서버에 대한 자세한 내용은 를 참조하십시오 "Cisco UCS C220 M5 랙 서버 데이터 시트".

C220 M5 랙 서버용 Cisco UCS VIC 1457 연결

다음 그림에 표시된 Cisco UCS VIC 1457 어댑터는 M5 세대의 Cisco UCS C-Series 서버용으로 설계된 4중 포트 소형 폼 팩터 플러그 가능(SFP28) 모듈식 마더보드 LAN(mLOM) 카드입니다. 이 카드는 10/25Gbps 이더넷 또는 FCoE를 지원합니다. 이 카드는 PCIe 표준 호환 인터페이스를 호스트에 제공할 수 있으며, NIC 또는 HBA로 동적으로 구성할 수 있습니다.

[오류: 그래픽 이미지가 없습니다]

Cisco UCS VIC 1457 어댑터에 대한 자세한 내용은 를 참조하십시오 "Cisco UCS 가상 인터페이스 카드 1400 시리즈 데이터 시트".

VMware vSphere 6.7U2

VMware vSphere 6.7U2는 FlexPod Express에서 사용할 수 있는 하이퍼바이저 옵션 중 하나입니다. VMware vSphere를 사용하면 구입한 컴퓨팅 용량을 최대한 활용하는 동시에 전력 및 냉각 설치 공간을 줄일 수 있습니다. 또한 VMware vSphere를 사용하면 vSphere 호스트 클러스터(유지 관리 모드의 VMware Distributed Resource Scheduler 또는 VMware DRS-MM)에서 하드웨어 장애 보호(VMware High Availability 또는 VMware HA)와 컴퓨팅 리소스 로드 밸런싱을 수행할 수 있습니다.

커널만 다시 시작하므로 VMware vSphere 6.7U2를 사용하면 하드웨어를 다시 시작하지 않고도 vSphere ESXi를 로드하여 빠르게 부팅할 수 있습니다. vSphere 6.7U2 vSphere 클라이언트(HTML5 기반 클라이언트)에는 코드 캡처 및 API 탐색을 지원하는 개발자 센터와 같은 몇 가지 새로운 개선 사항이 있습니다. 코드 캡처를 사용하면 vSphere Client에 작업을 기록하여 간단하고 사용 가능한 코드 출력을 제공할 수 있습니다. vSphere 6.7U2에는 DRS와 같은 새로운 기능이 유지 보수 모드(DRS-mm)에 포함되어 있습니다.

VMware vSphere 6.7U2는 다음과 같은 기능을 제공합니다.

- VMware는 외부 VMware PSC(Platform Services Controller) 구축 모델을 더 이상 사용하지 않습니다.

> ⓘ 다음 주요 vSphere 릴리즈부터는 외부 PSC를 사용할 수 없습니다.

- vCenter Server 어플라이언스 백업 및 복구를 위한 새로운 프로토콜 지원 지원되는 프로토콜 선택 사항으로 NFS 및 SMB 소개, 최대 총 7개(HTTP, HTTPS, FTP, FTPS, SCP, NFS 및 SMB) - 파일 기반 백업 또는 복구 작업을 위해 vCenter Server를 구성할 때 필요합니다.
- 콘텐츠 라이브러리 사용 시 새로운 기능. 이제 vCenter Server가 향상된 연결 모드로 구성되어 있으면 컨텐츠 라이브러리 간에 네이티브 VM 템플릿 동기화를 사용할 수 있습니다.
- 로 업데이트합니다 "클라이언트 플러그인 페이지".
- VMware vSphere Update Manager는 vSphere Client에도 향상된 기능을 추가합니다. 한 화면에서 연결 확인 규정 준수를 수행하고 조치를 수정할 수 있습니다.

VMware vSphere 6.7 U2에 대한 자세한 내용은 를 참조하십시오 "VMware vSphere 블로그 페이지를 참조하십시오".

VMware vCenter Server 6.7 U2 업데이트에 대한 자세한 내용은 를 참조하십시오 "릴리즈 노트".

이 솔루션은 vSphere 6.7U2에서 검증되었지만 에서 다른 구성 요소에 대해 검증된 모든 vSphere 버전을 지원합니다 "NetApp 상호 운용성 매트릭스 툴(IMT)". NetApp은 수정 및 향상된 기능을 위해 다음 버전의 vSphere를 구축할 것을 권장합니다.

부트 아키텍처

FlexPod 익스프레스 부트 아키텍처에서 지원되는 옵션은 다음과 같습니다.

- iSCSI SAN LUN 을 선택합니다
- Cisco FlexFlash SD 카드
- 로컬 디스크

FlexPod 데이터 센터는 iSCSI LUN에서 부팅되므로 FlexPod 익스프레스를 위한 iSCSI 부트를 사용하여 솔루션 관리성이 향상됩니다.

ESXi 호스트 가상 네트워크 인터페이스 카드 레이아웃

Cisco UCS VIC 1457에는 4개의 물리적 포트가 있습니다. 이 솔루션 검증에는 ESXi 호스트를 사용할 때 이러한 4개의 물리적 포트가 포함되어 있습니다. NIC 수가 더 작거나 큰 경우 VMNIC 번호가 다를 수 있습니다.

iSCSI 부트 구현에서 iSCSI 부트는 iSCSI 부트를 위해 별도의 vNIC(Virtual Network Interface Card)가 필요합니다. 이러한 vNIC는 적절한 패브릭의 iSCSI VLAN을 기본 VLAN으로 사용하며 다음 그림과 같이 iSCSI 부트 vSwitch에 연결됩니다.

[오류: 그래픽 이미지가 없습니다]

"다음: 결론."

결론

FlexPod Express의 검증된 설계는 업계 최고 수준의 구성 요소를 사용하는 간단하고 효율적인 솔루션입니다. FlexPod Express는 하이퍼바이저 플랫폼을 위한 확장 및 제공 옵션을 제공하여 특정 비즈니스 요구에 맞게 조정할 수 있습니다. FlexPod Express는 중소 및 중견 기업, 원격 사무소, 지사 및 전용 솔루션이 필요한 기타 기업을 위해 설계되었습니다.

"다음: 추가 정보를 찾을 위치."

추가 정보를 찾을 수 있는 위치

이 문서에 설명된 정보에 대한 자세한 내용은 다음 문서 및 웹 사이트를 참조하십시오.

- AFF and FAS 시스템 설명서 센터 를 참조하십시오

  "https://docs.netapp.com/platstor/index.jsp"

- AFF 문서 리소스 페이지

  "https://www.netapp.com/us/documentation/all-flash-fas.aspx"

- FlexPod Express with VMware vSphere 6.7 및 NetApp AFF C190 구축 가이드(진행 중)
- NetApp 설명서

  "https://docs.netapp.com"

FlexPod Express with Cisco UCS C-Series 및 NetApp AFF C190 Series 구축 가이드 를 참조하십시오

NVA-1142-deploy: FlexPod Express with Cisco UCS C-Series 및 NetApp AFF C190 Series-NVA Deployment

Savita Kumari, NetApp에서 기술 지원

업계 동향에 따르면 많은 데이터 센터가 공유 인프라 및 클라우드 컴퓨팅으로 전환하고 있습니다. 또한 기업에서는 데이터 센터에 친숙한 기술을 사용하는 원격 사무소 및 지사를 위해 간편하고 효율적인 솔루션을 찾고 있습니다.

FlexPod ® Express는 Cisco UCS(Cisco Unified Computing System), Cisco Nexus 스위치 제품군, NetApp ® 스토리지 기술을 기반으로 사전 설계되고 모범 사례 데이터 센터 아키텍처입니다. FlexPod 익스프레스 시스템의 구성요소는 FlexPod 데이터 센터와 비슷하기 때문에 더 작은 규모로 전체 IT 인프라 환경에서 관리 시너지 효과를 실현할 수 있습니다. FlexPod 데이터 센터 및 FlexPod 익스프레스는 가상화 및 베어 메탈 운영 체제 및 엔터프라이즈 워크로드를 위한 최적의 플랫폼입니다.

FlexPod 데이터 센터 및 FlexPod 익스프레스는 기본 구성을 제공하며 다양한 사용 사례 및 요구 사항을 수용할 수 있도록 크기를 조정할 수 있는 유연성을 갖추고 있습니다. 기존 FlexPod 데이터 센터 고객은 익숙한 툴을 사용하여 FlexPod 익스프레스 시스템을 관리할 수 있습니다. 새로운 FlexPod Express 고객은 환경 확장에 따라 FlexPod 데이터 센터 관리로 쉽게 전환할 수 있습니다.

FlexPod Express는 원격 사무소, 지점 및 중소기업을 위한 최적의 인프라 기반입니다. 전용 워크로드에 대한 인프라를 제공하려는 고객에게 최적의 솔루션입니다.

FlexPod Express는 거의 모든 워크로드에 적합한 관리하기 쉬운 인프라를 제공합니다.

솔루션 개요

이 FlexPod 익스프레스 솔루션은 FlexPod 통합 인프라 프로그램의 일부입니다.

FlexPod 통합 인프라 프로그램

FlexPod 참조 아키텍처는 CVD(Cisco Validated Design) 또는 NVA(NetApp Verified Architecture)로 제공됩니다. 지정된 CVD 또는 NVA의 고객 요구 사항에 따른 편차는 이러한 변형으로 지원되지 않는 구성이 생성되지는 않을 경우 허용됩니다.

FlexPod 프로그램에는 FlexPod 익스프레스 및 FlexPod 데이터 센터의 두 가지 솔루션이 포함되어 있습니다.

- * FlexPod 익스프레스. * 는 Cisco 및 NetApp의 기술을 갖춘 엔트리 레벨 솔루션을 고객에게 제공합니다.
- * FlexPod 데이터 센터 * 는 다양한 워크로드 및 애플리케이션을 위한 최적의 다목적 토대를 제공합니다.

NetApp 검증 아키텍처 프로그램

NetApp 검증 아키텍처 프로그램에서는 NetApp 솔루션을 위한 검증된 아키텍처를 고객에게 제공합니다. NetApp 검증 아키텍처는 다음과 같은 품질의 NetApp 솔루션 아키텍처를 제공합니다.

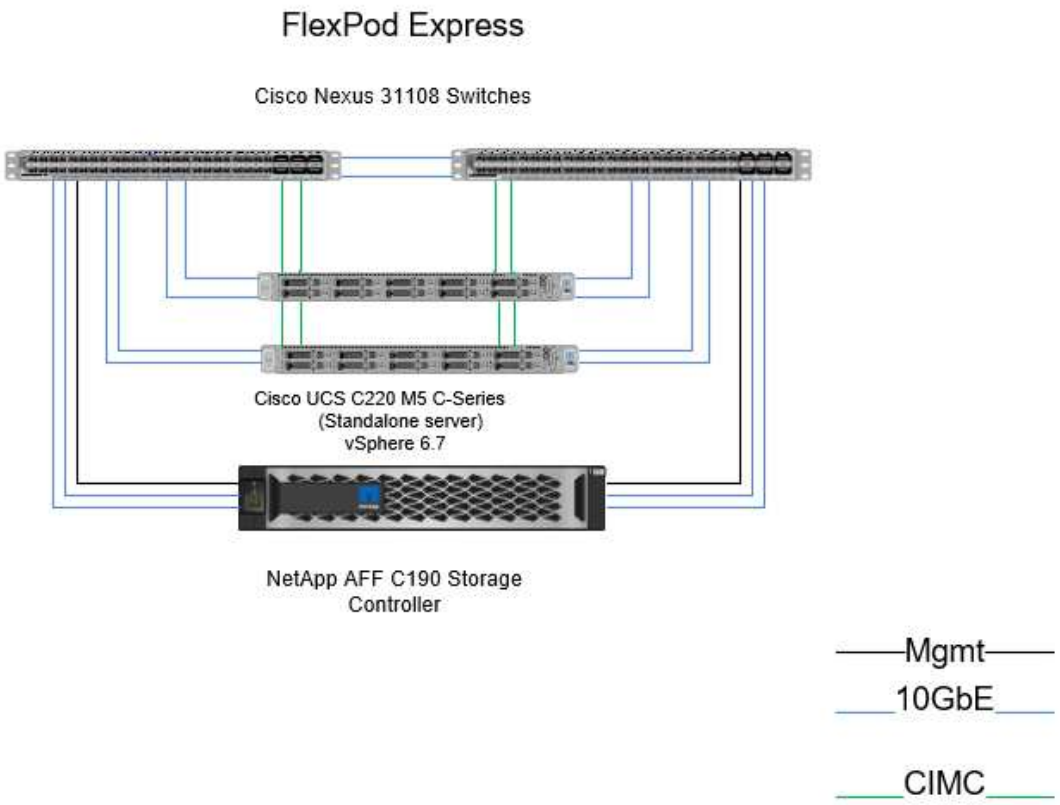
- 철저한 테스트
- 기본적으로 규범적인 아키텍처
- 구축 위험 최소화
- 시장 출시 기간 단축

이 가이드에서는 VMware vSphere를 사용한 FlexPod Express 설계에 대해 자세히 설명합니다. 또한 이 설계에서는 완전히 새로운 AFF C190 시스템(NetApp ONTAP ® 9.6 실행), Cisco Nexus 31108 및 Cisco UCS C-Series C220 M5 서버를 하이퍼바이저 노드로 사용합니다.

솔루션 기술

이 솔루션은 NetApp, Cisco 및 VMware의 최신 기술을 활용합니다. 이 솔루션에는 ONTAP 9.6, 이중 Cisco Nexus

31108 스위치 및 VMware vSphere 6.7U2를 실행하는 Cisco UCS C220 M5 랙 서버를 실행하는 새로운 NetApp AFF C190이 포함되어 있습니다. 이 검증된 솔루션은 10GbE 기술을 사용합니다. 또한 FlexPod 익스프레스 아키텍처가 조직의 변화하는 비즈니스 요구에 적응할 수 있도록 한 번에 두 개의 하이퍼바이저 노드를 추가하여 컴퓨팅 용량을 확장하는 방법에 대한 지침도 제공됩니다.



VIC 1457에서 4개의 물리적 10GbE 포트를 효율적으로 사용하려면 각 서버에서 상단 랙 스위치까지 2개의 추가 링크를 생성하십시오.

사용 사례 요약

FlexPod 익스프레스 솔루션은 다음과 같은 여러 사용 사례에 적용할 수 있습니다.

- 원격 사무소 또는 지점 사무소
- 중소기업
- 비용 효율적인 전용 솔루션이 필요한 환경

FlexPod Express는 가상화된 혼합 워크로드에 가장 적합합니다. 이 솔루션은 vSphere 6.7U2에서 검증되었지만 NetApp Interoperability Matrix Tool에 의해 다른 구성 요소와 함께 검증된 모든 vSphere 버전을 지원합니다. 다음과 같은 수정 사항 및 향상된 기능 때문에 vSphere 6.7U2를 구축하는 것이 좋습니다.

- HTTP, HTTPS, FTP, FTPS 등 vCenter Server Appliance 백업 및 복원을 위한 새로운 프로토콜 지원 SCP, NFS 및 SMB
- 콘텐츠 라이브러리를 활용할 때 새로운 기능을 제공합니다. 이제 vCenter Server가 향상된 연결 모드로 구성되어

있으면 컨텐츠 라이브러리 간에 네이티브 VM 템플릿을 동기화할 수 있습니다.

- 업데이트된 클라이언트 플러그인 페이지.
- VUM(vSphere Update Manager) 및 vSphere Client에 향상된 기능이 추가되었습니다. 이제 한 화면에서 연결, 규정 준수 확인 및 수정 작업을 모두 수행할 수 있습니다.

이 주제에 대한 자세한 내용은 를 참조하십시오 "vSphere 6.7U2 페이지" 및 "vCenter Server 6.7U2 릴리즈 노트".

기술 요구 사항

FlexPod 익스프레스 시스템에는 하드웨어 및 소프트웨어 구성 요소의 조합이 필요합니다. 또한 FlexPod Express는 하이퍼바이저 노드를 시스템에 추가하는 데 필요한 하드웨어 구성요소를 2개 단위로 설명합니다.

하드웨어 요구 사항

선택한 하이퍼바이저에 관계없이 모든 FlexPod Express 구성은 동일한 하드웨어를 사용합니다. 따라서 비즈니스 요구사항이 변경되더라도 동일한 FlexPod Express 하드웨어에서 다른 하이퍼바이저를 사용할 수 있습니다.

다음 표에는 FlexPod Express 구성 및 구축에 필요한 하드웨어 구성요소가 나와 있습니다. 솔루션 구현에 사용되는 하드웨어 구성요소는 고객 요구사항에 따라 다를 수 있습니다.

하드웨어	수량
AFF C190 2노드 클러스터	1
Cisco C220 M5 서버	2
Cisco Nexus 31108PC-V 스위치	2
Cisco UCS C220 M5 랙 서버용 Cisco UCS VIC(가상 인터페이스 카드) 1457	2

이 표에는 10GbE 구현을 위한 기본 구성 외에 필요한 하드웨어가 나와 있습니다.

하드웨어	수량
Cisco UCS C220 M5 서버	2
Cisco VIC 1457	2

소프트웨어 요구 사항

다음 표에는 FlexPod 익스프레스 솔루션의 아키텍처를 구현하는 데 필요한 소프트웨어 구성 요소가 나열되어 있습니다.

소프트웨어	버전	세부 정보
CIMC(Cisco Integrated Management Controller)	4.0.4	Cisco UCS C220 M5 랙 서버용
Cisco nenic 드라이버	1.0.0.29	VIC 1457 인터페이스 카드용
Cisco NX-OS입니다	7.0(3) i7(6)	Cisco Nexus 31108PC-V 스위치용
NetApp ONTAP를 참조하십시오	9.6	AFF C190 컨트롤러의 경우

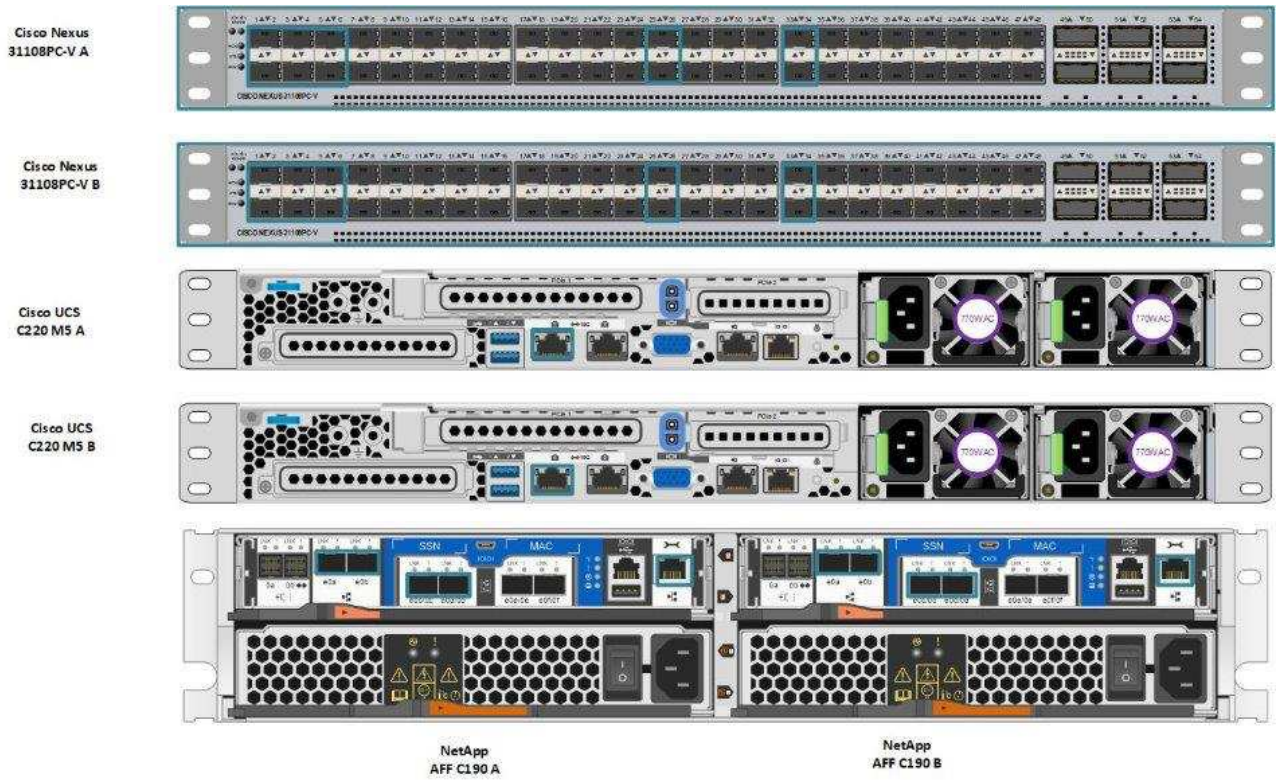
이 표에는 FlexPod Express의 모든 VMware vSphere 구축에 필요한 소프트웨어가 나열되어 있습니다.

소프트웨어	버전
VMware vCenter Server 어플라이언스	6.7U2
VMware vSphere ESXi 하이퍼바이저	6.7U2
ESXi용 NetApp VAAI 플러그인	1.1.2
NetApp VSC를 기반으로 합니다	9.6

FlexPod Express 케이블링 정보

이 참조 검증은 다음 그림 및 표와 같이 케이블로 연결됩니다.

이 그림은 참조 검증 케이블 연결을 보여 줍니다.



다음 표에는 Cisco Nexus 스위치 31108PC-V-A의 케이블 연결 정보가 나와 있습니다

로컬 장치	로컬 포트	원격 장치	원격 포트
Cisco Nexus 스위치 31108PC-V A	eth1/1	NetApp AFF C190 스토리지 컨트롤러 A	e0c
	eth1/2	NetApp AFF C190 스토리지 컨트롤러 B	e0c
	eth1/3	Cisco UCS C220 C-Series 독립 실행형 서버 A	MLOM0
	eth1/4	Cisco UCS C220 C-Series 독립 실행형 서버 B	MLOM0
	eth1/5	Cisco UCS C220 C-Series 독립 실행형 서버 A	MLOM1
	eth1/6	Cisco UCS C220 C-Series 독립 실행형 서버 B	MLOM1
	eth1/25	Cisco Nexus 스위치 31108PC-V B	eth1/25
	Eth1/26	Cisco Nexus 스위치 31108PC-V B	Eth1/26
	Eth1/33	NetApp AFF C190 스토리지 컨트롤러 A	e0M
	eth1/34	Cisco UCS C220 C-Series 독립 실행형 서버 A	CIMC(FEX135/1/25)

이 표에는 Cisco Nexus 스위치 31108PC-V-B의 케이블 연결 정보가 나와 있습니다

로컬 장치	로컬 포트	원격 장치	원격 포트
Cisco Nexus 스위치 31108PC-V B	eth1/1	NetApp AFF C190 스토리지 컨트롤러 A	e0d
	eth1/2	NetApp AFF C190 스토리지 컨트롤러 B	e0d
	eth1/3	Cisco UCS C220 C-Series 독립 실행형 서버 A	MLOM2
	eth1/4	Cisco UCS C220 C-Series 독립 실행형 서버 B	MLOM2
	eth1/5	Cisco UCS C220 C-Series 독립 실행형 서버 A	MLOM3
	eth1/6	Cisco UCS C220 C-Series 독립 실행형 서버 B	MLOM3
	eth1/25	Cisco Nexus 스위치 31108 A	eth1/25
	Eth1/26	Cisco Nexus 스위치 31108 A	Eth1/26
	Eth1/33	NetApp AFF C190 스토리지 컨트롤러 B	e0M
	eth1/34	Cisco UCS C220 C-Series 독립 실행형 서버 B	CIMC(FEX135/1/26)

이 표에는 NetApp AFF C190 스토리지 컨트롤러 A의 케이블 연결 정보가 나와 있습니다

로컬 장치	로컬 포트	원격 장치	원격 포트
NetApp AFF C190 스토리지 컨트롤러 A	e0a	NetApp AFF C190 스토리지 컨트롤러 B	e0a
	e0b	NetApp AFF C190 스토리지 컨트롤러 B	e0b
	e0c	Cisco Nexus 스위치 31108PC-V A	eth1/1
	e0d	Cisco Nexus 스위치 31108PC-V B	eth1/1
	e0M	Cisco Nexus 스위치 31108PC-V A	Eth1/33

이 표에는 NetApp AFF C190 스토리지 컨트롤러 B의 케이블 연결 정보가 나와 있습니다

로컬 장치	로컬 포트	원격 장치	원격 포트
NetApp AFF C190 스토리지 컨트롤러 B	e0a	NetApp AFF C190 스토리지 컨트롤러 A	e0a
	e0b	NetApp AFF C190 스토리지 컨트롤러 A	e0b
	e0c	Cisco Nexus 스위치 31108PC-V A	eth1/2
	e0d	Cisco Nexus 스위치 31108PC-V B	eth1/2
	e0M	Cisco Nexus 스위치 31108PC-V B	Eth1/33

구현 절차

개요

이 문서에서는 완전히 이중화된 고가용성 FlexPod Express 시스템을 구성하는 방법에 대해 자세히 설명합니다. 이러한 이중화를 반영하기 위해 각 단계에서 구성 요소를 구성 요소 A 또는 구성 요소 B라고 합니다 예를 들어 컨트롤러 A와 컨트롤러 B는 이 문서에 프로비저닝된 NetApp 스토리지 컨트롤러 2개를 식별합니다. 스위치 A와 스위치 B는 Cisco Nexus 스위치 쌍을 나타냅니다.

또한 서버 A, 서버 B 등으로 순차적으로 구분되는 여러 Cisco UCS 호스트를 프로비저닝하는 단계도 설명합니다.

사용자 환경과 관련된 정보를 단계별로 포함해야 함을 나타내기 위해 명령 구조의 일부로 '<<text>>'이 표시됩니다. 'VLAN create' 명령은 다음 예를 참조하십시오.

```
Controller01> network port vlan create -node <<var_nodeA>> -vlan-name
<<var_vlan-name>>
```

이 문서를 사용하여 FlexPod Express 환경을 완전히 구성할 수 있습니다. 이 프로세스에서 다양한 단계를 수행하려면 고객별 명명 규칙, IP 주소 및 VLAN(Virtual Local Area Network) 스키마를 삽입해야 합니다. 다음 표에서는 이 가이드에 설명된 대로 구축에 필요한 VLAN을 설명합니다. 이 표는 특정 사이트 변수를 기반으로 완료할 수 있으며 문서 구성 단계를 구현하는 데 사용할 수 있습니다.

별도의 대역내 및 대역외 관리 VLAN을 사용하는 경우 이러한 VLAN 간에 레이어 3 경로를 만들어야 합니다. 이 검증에서는 공통 관리 VLAN이 사용되었습니다.

VLAN 이름입니다	**VLAN**의 용도	**VLAN ID**입니다	
관리 VLAN	관리 인터페이스용 VLAN	3437	vSwitch0
NFS VLAN	NFS 트래픽용 VLAN	3438	vSwitch0

VLAN 이름입니다	**VLAN**의 용도	**VLAN ID**입니다	
VMware vMotion VLAN	가상 머신(VM)을 하나의 물리적 호스트에서 다른 물리적 호스트로 이동하도록 지정된 VLAN	3441	vSwitch0
VM 트래픽 VLAN	VM 애플리케이션 트래픽용 VLAN	3442	vSwitch0
iSCSI-A-VLAN	패브릭 A의 iSCSI 트래픽용 VLAN	3439	iSciBootvSwitch
iSCSI-B-VLAN	패브릭 B의 iSCSI 트래픽용 VLAN	3440	iSciBootvSwitch
네이티브 VLAN	태그가 지정되지 않은 프레임이 할당되는 VLAN입니다	2	

FlexPod Express를 구성하는 동안 VLAN 번호가 필요합니다. VLAN은 "<<var_xxxx_vlan>>"라고 하며, 여기서 "xxxx"는 VLAN의 목적(예: iSCSI-A)입니다.

이 검증에는 두 개의 vSwitch가 생성됩니다.

다음 표에는 솔루션 vSwitch가 나와 있습니다.

vSwitch 이름입니다	활성 어댑터	포트	**MTU**	로드 밸런싱
vSwitch0	Vmnic2, vmnic4	기본값(120)	9000입니다	IP 해시를 기반으로 하는 라우트입니다
iSciBootvSwitch	Vmnic3, vmnic5	기본값(120)	9000입니다	발신 가상 포트 ID를 기반으로 하는 라우트입니다.

로드 밸런싱의 IP 해시 방법을 사용하려면 정적(모드 켜짐) 포트 채널과 함께 SRC-DST-IP EtherChannel을 사용하는 기본 물리적 스위치에 대해 적절한 구성이 필요합니다. 스위치 구성이 잘못되어 연결이 간헐적으로 이루어지는 경우 포트 채널 설정 문제를 해결하는 동안 ESXi 관리 vmkernel 포트와의 통신을 복구하기 위해 Cisco 스위치에서 연결된 두 개의 업링크 포트 중 하나를 일시적으로 종료합니다.

다음 표에는 생성된 VMware VM이 나와 있습니다.

VM 설명입니다	호스트 이름입니다
VMware vCenter Server를 참조하십시오	FlexPod-VCSA를 참조하십시오
가상 스토리지 콘솔	FlexPod-VSC를 참조하십시오

Cisco Nexus 31108PC-V 구축

이 섹션에서는 FlexPod 익스프레스 환경에서 사용되는 Cisco Nexus 331108PC-V 스위치 구성에 대해 자세히 설명합니다.

Cisco Nexus 31108PC-V 스위치의 초기 설정

다음 절차에서는 기본 FlexPod Express 환경에서 사용할 Cisco Nexus 스위치를 구성하는 방법에 대해 설명합니다.

> 이 절차에서는 NX-OS 소프트웨어 릴리즈 7.0(3) i7(6)을 실행하는 Cisco Nexus 31108PC-V를 사용하고 있다고 가정합니다.

1. 초기 부팅이 완료되고 스위치의 콘솔 포트에 연결되면 Cisco NX-OS 설정이 자동으로 시작됩니다. 이 초기 구성에서는 스위치 이름, mgmt0 인터페이스 구성, SSH(Secure Shell) 설정과 같은 기본 설정을 지정합니다.
2. FlexPod 익스프레스 관리 네트워크는 여러 가지 방법으로 구성할 수 있습니다. 31108PC-V 스위치의 mgmt0 인터페이스를 기존 관리 네트워크에 연결할 수도 있고, 31108PC-V 스위치의 mgmt0 인터페이스를 연속 연결 구성으로 연결할 수도 있습니다. 하지만 이 링크는 SSH 트래픽과 같은 외부 관리 액세스에 사용할 수 없습니다.

   > 이 구축 가이드에서는 FlexPod Express Cisco Nexus 31108PC-V 스위치가 기존 관리 네트워크에 연결되어 있습니다.

3. Cisco Nexus 31108PC-V 스위치를 구성하려면 스위치 전원을 켜고 화면 메시지에 따라 두 스위치를 초기 설정하고 스위치 관련 정보에 해당하는 값을 대체합니다.

```
This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.
*Note: setup is mainly used for configuring the system initially,
when no configuration is present. So setup always assumes system
defaults and not the current system configuration values.
Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.
Would you like to enter the basic configuration dialog (yes/no): y
Do you want to enforce secure password standard (yes/no) [y]: y
  Create another login account (yes/no) [n]: n
  Configure read-only SNMP community string (yes/no) [n]: n
  Configure read-write SNMP community string (yes/no) [n]: n
  Enter the switch name : 31108PC-V-B
  Continue with Out-of-band (mgmt0) management configuration? (yes/no)
[y]: y
    Mgmt0 IPv4 address : <<var_switch_mgmt_ip>>
    Mgmt0 IPv4 netmask : <<var_switch_mgmt_netmask>>
  Configure the default gateway? (yes/no) [y]: y
    IPv4 address of the default gateway : <<var_switch_mgmt_gateway>>
  Configure advanced IP options? (yes/no) [n]: n
  Enable the telnet service? (yes/no) [n]: n
  Enable the ssh service? (yes/no) [y]: y
    Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa
    Number of rsa key bits <1024-2048> [1024]: <enter>
  Configure the ntp server? (yes/no) [n]: y
    NTP server IPv4 address : <<var_ntp_ip>>
  Configure default interface layer (L3/L2) [L2]: <enter>
  Configure default switchport interface state (shut/noshut) [noshut]:
<enter>
  Configure CoPP system profile (strict/moderate/lenient/dense)
[strict]: <enter>
```

4. 그러면 구성 요약이 표시됩니다. 구성을 편집할지 묻는 메시지가 나타납니다. 구성이 올바르면 n을 입력합니다.

```
Would you like to edit the configuration? (y
es/no) [n]: n
```

5. 그런 다음 이 구성을 사용하고 저장할지 묻는 메시지가 표시됩니다. 그렇다면 y를 입력합니다.

```
Use this configuration and save it? (yes/no) [y]: Enter
```

6. Cisco Nexus 스위치 B에 대해 이 절차를 반복합니다

고급 기능을 활성화합니다

추가 구성 옵션을 제공하려면 Cisco NX-OS에서 특정 고급 기능을 사용하도록 설정해야 합니다. Cisco Nexus 스위치 A 및 스위치 B에서 적절한 기능을 사용하도록 설정하려면 명령(config t)을 사용하여 구성 모드를 시작하고 다음 명령을 실행합니다.

```
feature interface-vlan
feature lacp
feature vpc
```

기본 포트 채널 로드 밸런싱 해쉬는 소스 및 타깃 IP 주소를 사용하여 포트 채널의 인터페이스에 대한 로드 밸런싱 알고리즘을 결정합니다. 소스 및 타깃 IP 주소보다 많은 입력을 해쉬 알고리즘에 제공하면 포트 채널 멤버 전체에 걸쳐 더 효율적으로 분산될 수 있습니다. 동일한 이유로 소스 및 타깃 TCP 포트를 해쉬 알고리즘에 추가하는 것이 좋습니다.

구성 모드(config t)에서 다음 명령을 입력하여 Cisco Nexus 스위치 A 및 스위치 B의 글로벌 포트 채널 로드 밸런싱 구성을 설정하십시오.

```
port-channel load-balance src-dst ip-l4port
```

글로벌 스패닝 트리를 구성합니다

Cisco Nexus 플랫폼은 브리지 보장이라는 새로운 보호 기능을 사용합니다. 브리지 보장은 스패닝 트리 알고리즘을 더 이상 실행하지 않는 장치에서 데이터 트래픽을 계속 전달하는 단방향 링크 또는 기타 소프트웨어 장애를 방지합니다. 플랫폼에 따라 네트워크 또는 가장자리를 포함한 여러 상태 중 하나에 포트를 배치할 수 있습니다.

기본적으로 모든 포트가 네트워크 포트로 간주되도록 브리지 보장을 설정하는 것이 좋습니다. 이 설정은 네트워크 관리자가 각 포트의 구성을 검토하도록 합니다. 또한 확인되지 않은 에지 포트 또는 브리지 보장 기능이 활성화되지 않은 인접 장치와 같은 가장 일반적인 구성 오류도 표시됩니다. 또한 스패닝 트리에서 너무 적은 포트가 아니라 많은 포트를 차단하는 편이 더 안전합니다. 그러면 기본 포트 상태를 통해 네트워크의 전반적인 안정성을 향상할 수 있습니다.

특히 브리지 보장을 지원하지 않는 서버, 스토리지 및 업링크 스위치를 추가할 때는 스패닝 트리 상태에 세심한 주의를 기울여야 합니다. 이러한 경우 포트를 활성화하려면 포트 유형을 변경해야 할 수 있습니다.

브리지 프로토콜 데이터 단위(BPDU) 보호대는 기본적으로 다른 보호 계층으로 에지 포트에서 활성화됩니다. 네트워크의 루프를 방지하기 위해 이 기능은 다른 스위치의 BPDU가 이 인터페이스에 표시되는 경우 포트를 종료합니다.

구성 모드(config t)에서 다음 명령을 실행하여 Cisco Nexus 스위치 A 및 스위치 B에서 기본 포트 유형과 BPDU 가드를 포함한 기본 스패닝 트리 옵션을 구성하십시오.

```
spanning-tree port type network default
spanning-tree port type edge bpduguard default
spanning-tree port type edge bpdufilter default
ntp server <<var_ntp_ip>> use-vrf management
ntp master 3
```

VLAN을 정의합니다

VLAN이 서로 다른 개별 포트를 구성하기 전에 스위치에서 레이어 2 VLAN을 정의해야 합니다. 향후 문제 해결이 용이하도록 VLAN 이름을 지정하는 것도 좋은 방법입니다.

구성 모드(config t)에서 다음 명령을 실행하여 Cisco Nexus 스위치 A 및 스위치 B의 계층 2 VLAN을 정의하고 설명하십시오.

```
vlan <<nfs_vlan_id>>
  name NFS-VLAN
vlan <<iSCSI_A_vlan_id>>
  name iSCSI-A-VLAN
vlan <<iSCSI_B_vlan_id>>
  name iSCSI-B-VLAN
vlan <<vmotion_vlan_id>>
  name vMotion-VLAN
vlan <<vmtraffic_vlan_id>>
  name VM-Traffic-VLAN
vlan <<mgmt_vlan_id>>
  name MGMT-VLAN
vlan <<native_vlan_id>>
  name NATIVE-VLAN
exit
```

액세스 및 관리 포트 설명을 구성합니다

레이어 2 VLAN에 이름을 할당하는 경우와 마찬가지로, 모든 인터페이스에 대한 설정 설명은 프로비저닝과 문제 해결에 도움이 될 수 있습니다.

각 스위치의 구성 모드(config t)에서 FlexPod Express 대규모 구성에 대한 다음 포트 설명을 입력합니다.

Cisco Nexus 스위치 **A**

```
int eth1/1
  description AFF C190-A e0c
int eth1/2
  description AFF C190-B e0c
int eth1/3
  description UCS-Server-A: MLOM port 0 vSwitch0
int eth1/4
  description UCS-Server-B: MLOM port 0 vSwitch0
int eth1/5
  description UCS-Server-A: MLOM port 1 iScsiBootvSwitch
int eth1/6
  description UCS-Server-B: MLOM port 1 iScsiBootvSwitch
int eth1/25
  description vPC peer-link 31108PC-V-B 1/25
int eth1/26
  description vPC peer-link 31108PC-V-B 1/26
int eth1/33
  description AFF C190-A e0M
int eth1/34
  description UCS Server A: CIMC
```

Cisco Nexus 스위치 B

```
int eth1/1
  description AFF C190-A e0d
int eth1/2
  description AFF C190-B e0d
int eth1/3
  description UCS-Server-A: MLOM port 2 vSwitch0
int eth1/4
description UCS-Server-B: MLOM port 2 vSwitch0
int eth1/5
  description UCS-Server-A: MLOM port 3 iScsiBootvSwitch
int eth1/6
  description UCS-Server-B: MLOM port 3 iScsiBootvSwitch
int eth1/25
  description vPC peer-link 31108PC-V-A 1/25
int eth1/26
  description vPC peer-link 31108PC-V-A 1/26
int eth1/33
  description AFF C190-B e0M
int eth1/34
  description UCS Server B: CIMC
```

서버 및 스토리지 관리 인터페이스를 구성합니다

서버와 스토리지 모두의 관리 인터페이스는 일반적으로 단일 VLAN만 사용합니다. 따라서 관리 인터페이스 포트를 액세스 포트로 구성합니다. 각 스위치에 대한 관리 VLAN을 정의하고 스패닝 트리 포트 유형을 에지로 변경합니다.

구성 모드(config t)에서 다음 명령을 입력하여 서버와 스토리지 모두의 관리 인터페이스에 대한 포트 설정을 구성하십시오.

Cisco Nexus 스위치 **A**

```
int eth1/33-34
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

Cisco Nexus 스위치 **B**

```
int eth1/33-34
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

가상 포트 채널 글로벌 구성을 수행합니다

가상 포트 채널(vPC)을 사용하면 물리적으로 두 개의 서로 다른 Cisco Nexus 스위치에 연결된 링크가 세 번째 장치에 단일 포트 채널로 표시될 수 있습니다. 세 번째 장치는 스위치, 서버 또는 다른 네트워킹 장치일 수 있습니다. vPC는 계층 2 다중 경로를 제공할 수 있으므로 대역폭을 높이고, 노드 간에 여러 개의 병렬 경로를 활성화하고, 대체 경로가 있는 로드 밸런싱 트래픽을 통해 이중화를 생성할 수 있습니다.

vPC는 다음과 같은 이점을 제공합니다.

- 단일 장치에서 두 업스트림 장치에 걸쳐 포트 채널을 사용하도록 설정
- 스패닝 트리 프로토콜 차단 포트 제거
- 루프 없는 토폴로지 제공
- 사용 가능한 모든 업링크 대역폭 사용
- 링크 또는 디바이스에 장애가 발생할 경우 빠른 컨버전스를 제공합니다
- 링크 레벨의 복원력 제공
- 고가용성 제공 지원

vPC 기능이 제대로 작동하려면 두 Cisco Nexus 스위치 간의 몇 가지 초기 설정이 필요합니다. 연속 인접 mgmt0 구성을 사용하는 경우에는 인터페이스에 정의된 주소를 사용하고 "ping"\< 스위치_A/B_mgmt0_ip_addr>>VRF" 관리

명령을 사용하여 통신 가능 여부를 확인해야 합니다.

구성 모드(config t)에서 다음 명령을 실행하여 두 스위치에 대한 vPC 글로벌 구성을 설정하십시오.

Cisco Nexus 스위치 **A**

```
vpc domain 1
 role priority 10
  peer-keepalive destination <<switch_B_mgmt0_ip_addr>> source
<<switch_A_mgmt0_ip_addr>> vrf
management
peer-switch
peer-gateway
auto-recovery
delay restore 150
ip arp synchronize
int eth1/25-26
  channel-group 10 mode active
int Po10
  description vPC peer-link
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type network
  vpc peer-link
  no shut
exit
copy run start
```

Cisco Nexus 스위치 **B**

```
vpc domain 1
  peer-switch
  role priority 20
  peer-keepalive destination <<switch_A_mgmt0_ip_addr>> source
<<switch_B_mgmt0_ip_addr>> vrf management
  peer-gateway
  auto-recovery
  delay-restore 150
   ip arp synchronize
int eth1/25-26
  channel-group 10 mode active
int Po10
  description vPC peer-link
  switchport
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type network
  vpc peer-link
no shut
exit
copy run start
```

스토리지 포트 채널을 구성합니다

NetApp 스토리지 컨트롤러는 LACP(Link Aggregation Control Protocol)를 사용하여 네트워크에 대해 active-active 연결을 허용합니다. LACP 사용이 선호되는 이유는 LACP가 스위치 간에 협상과 로깅을 모두 추가하기 때문입니다. 네트워크가 vPC에 맞게 설정되므로 이 접근 방식을 통해 스토리지에서 별도의 물리적 스위치로의 active-active 연결을 설정할 수 있습니다. 각 컨트롤러에는 각 스위치에 대한 링크가 2개 있습니다. 하지만 4개의 모든 링크는 동일한 vPC 및 인터페이스 그룹(ifgrp)의 일부입니다.

구성 모드(config t)에서 각 스위치에 대해 다음 명령을 실행하여 개별 인터페이스를 구성하고 NetApp AFF 컨트롤러에 연결된 포트에 대한 결과 포트 채널 구성을 설정하십시오.

1. 스위치 A와 스위치 B에서 다음 명령을 실행하여 스토리지 컨트롤러 A의 포트 채널을 구성합니다.

```
int eth1/1
  channel-group 11 mode active
int Po11
  description vPC to Controller-A
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<nfs_vlan_id>>,<<mgmt_vlan_id>>,<<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  vpc 11
  no shut
```

2. 스위치 A와 스위치 B에서 다음 명령을 실행하여 스토리지 컨트롤러 B의 포트 채널을 구성합니다.

```
int eth1/2
  channel-group 12 mode active
int Po12
  description vPC to Controller-B
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<mgmt_vlan_id>>,
<<iSCSI_A_vlan_id>>, <<iSCSI_B_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  vpc 12
  no shut
exit
copy run start
```

서버 연결을 구성합니다

Cisco UCS 서버에는 데이터 트래픽과 iSCSI를 사용한 ESXi 운영 체제 부팅에 사용되는 4포트 가상 인터페이스 카드 VIC1457이 있습니다. 이러한 인터페이스는 서로 간에 페일오버되도록 구성되어 단일 링크를 넘어 추가적인 이중화를 제공합니다. 이러한 링크를 여러 스위치에 걸쳐 분산하면 완전한 스위치 장애가 발생해도 서버가 가동 상태를 유지할 수 있습니다.

구성 모드(config t)에서 다음 명령을 실행하여 각 서버에 연결된 인터페이스에 대한 포트 설정을 구성하십시오.

Cisco Nexus 스위치 **A: Cisco UCS** 서버 **A** 및 **Cisco UCS** 서버 **B** 구성

```
int eth1/5
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<iSCSI_A_vlan_id>>,<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_i
d>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  no shut
exit
copy run start
```

Cisco Nexus 스위치 **B: Cisco UCS** 서버 **A** 및 **Cisco UCS** 서버 **B** 구성

```
int eth1/6
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<iSCSI_B_vlan_id>>,<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_i
d>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  no shut
exit
copy run start
```

서버 포트 채널을 구성합니다

스위치 A와 스위치 B에서 다음 명령을 실행하여 서버 A에 대한 포트 채널을 구성합니다.

```
int eth1/3
  channel-group 13 mode active
int Po13
  description vPC to Server-A
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_id>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  vpc 13
  no shut
```

스위치 A와 스위치 B에서 다음 명령을 실행하여 서버 B에 대한 포트 채널을 구성합니다.

```
int eth1/4
  channel-group 14 mode active
int Po14
  description vPC to Server-B
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_id>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  vpc 14
  no shut
```

이 솔루션 검증에 9000의 MTU가 사용되었습니다. 그러나 애플리케이션 요구 사항에 적합한 MTU에 대해 다른 값을 구성할 수 있습니다. FlexPod 솔루션에서 동일한 MTU 값을 설정하는 것이 중요합니다. 구성 요소 간의 MTU 구성이 잘못되면 패킷이 손실되고 이러한 패킷은 다시 전송되어야 하며 솔루션의 전반적인 성능에 영향을 미칩니다.

Cisco UCS 서버를 추가하여 솔루션을 확장하거나, 스위치 A 및 B에서 새로 추가한 서버가 연결된 스위치 포트를 사용하여 이전 명령을 실행합니다

기존 네트워크 인프라로 업링크

사용 가능한 네트워크 인프라에 따라 여러 가지 방법과 기능을 사용하여 FlexPod 환경을 업링크할 수 있습니다. 기존 Cisco Nexus 환경이 존재하는 경우, NetApp은 vPC를 사용하여 FlexPod 환경에 포함된 Cisco Nexus 31108 스위치를 인프라로 업링크하는 것을 권장합니다. 업링크는 10GbE 인프라스트럭처 솔루션의 경우 10GbE 업링크, 필요한 경우 1GbE 인프라스트럭처 솔루션의 경우 1GbE가 될 수 있습니다. 앞서 설명한 절차를 사용하여 기존 환경에 대한 업링크 vPC를 생성할 수 있습니다. 구성이 완료된 후 각 스위치에 대한 구성을 저장하려면 copy start를 실행해야 합니다.

"다음은 NetApp 스토리지 구축 절차(1부)입니다."

NetApp 스토리지 구축 절차(1부)

이 섹션에서는 NetApp AFF 스토리지 구축 절차를 설명합니다.

NetApp 스토리지 컨트롤러 AFF C190 시리즈 설치

NetApp Hardware Universe를 참조하십시오

NetApp HWU(Hardware Universe) 애플리케이션은 특정 ONTAP 버전에 대해 지원되는 하드웨어 및 소프트웨어 구성요소를 제공합니다. 현재 ONTAP 소프트웨어가 지원하는 모든 NetApp 스토리지 어플라이언스에 대한 구성 정보를 제공합니다. 구성요소 호환성 표도 제공합니다.

사용하려는 하드웨어 및 소프트웨어 구성 요소가 설치하려는 ONTAP 버전에서 지원되는지 확인합니다.

에 액세스합니다 "HWU" 응용 프로그램 - 시스템 구성 가이드를 봅니다. 컨트롤러 탭을 클릭하여 원하는 사양의 ONTAP 소프트웨어 버전과 NetApp 스토리지 어플라이언스 간의 호환성을 확인하십시오.

또는 스토리지 어플라이언스별로 구성 요소를 비교하려면 스토리지 시스템 비교 를 클릭합니다.

컨트롤러 **AFFC190 Series** 사전 요구사항
스토리지 시스템의 물리적 위치를 계획하려면 NetApp Hardware Universe를 참조하십시오. 다음 섹션을 참조하십시오. • 전기 요구 사항 • 지원되는 전원 코드 • 온보드 포트 및 케이블

스토리지 컨트롤러

AFF의 컨트롤러에 대한 물리적 설치 절차를 따릅니다 "C190" 문서화:

NetApp ONTAP 9.6

구성 워크시트

설치 스크립트를 실행하기 전에 제품 설명서에서 구성 워크시트를 작성하십시오. 구성 워크시트는 ONTAP 9.6 소프트웨어 설치 가이드에서 사용할 수 있습니다.

이 시스템은 스위치가 없는 2노드 클러스터 구성에서 설정됩니다.

다음 표는 ONTAP 9.6 설치 및 구성 정보를 제공합니다.

클러스터 세부 정보	클러스터 세부 정보 값입니다
클러스터 노드 A IP 주소입니다	<<var_NodeA_mgmt_ip>> 를 입력합니다
클러스터 노드 A 넷마스크	<<var_NodeA_mgmt_mask>> 를 입력합니다
클러스터 노드 A 게이트웨이	<<var_NodeA_mgmt_gateway>> 를 참조하십시오
클러스터 노드 A 이름	<<var_NodeA>> 를 참조하십시오
클러스터 노드 B IP 주소입니다	<<var_NodeB_mgmt_ip>> 를 입력합니다
클러스터 노드 B 넷마스크	<<var_NodeB_mgmt_mask>> 를 입력합니다
클러스터 노드 B 게이트웨이	<<var_NodeB_mgmt_gateway>> 를 참조하십시오
클러스터 노드 B 이름	<<var_NodeB>> 를 참조하십시오
ONTAP 9.6 URL입니다	<<var_url_boot_software>>
클러스터의 이름입니다	<<var_clustername>> 를 클릭합니다
클러스터 관리 IP 주소입니다	<<var_clustermgmt_ip>> 를 입력합니다
클러스터 B 게이트웨이	<<var_clustermgmt_gateway>> 를 클릭합니다
클러스터 B 넷마스크	<<var_clustermgmt_mask>> 를 입력합니다

클러스터 세부 정보	클러스터 세부 정보 값입니다
도메인 이름	<<var_domain_name>>
DNS 서버 IP(둘 이상 입력할 수 있음)	var_dns_server_ip입니다
NTP 서버 IP(둘 이상 입력할 수 있음)	<<var_ntp_server_ip>> 를 참조하십시오

노드 **A**를 구성합니다

노드 A를 구성하려면 다음 단계를 완료하십시오.

1. 스토리지 시스템 콘솔 포트에 연결합니다. Loader-A 메시지가 표시됩니다. 하지만 스토리지 시스템이 재부팅 루프 상태인 경우 다음 메시지가 표시될 때 Ctrl-C를 눌러 자동 부팅 루프를 종료합니다.

   ```
   Starting AUTOBOOT press Ctrl-C to abort…
   ```

   시스템이 부팅되도록 합니다.

   ```
   autoboot
   ```

2. Ctrl-C를 눌러 부팅 메뉴로 들어갑니다.

   ⓘ ONTAP 9.6이 부팅 중인 소프트웨어 버전이 아닌 경우 다음 단계를 계속하여 새 소프트웨어를 설치하십시오. ONTAP 9.6이 부팅 중인 버전인 경우 옵션 8 및 y를 선택하여 노드를 재부팅합니다. 그런 다음 14단계를 계속합니다.

3. 새 소프트웨어를 설치하려면 옵션 7을 선택합니다.
4. 업그레이드를 수행하려면 y 를 입력합니다.
5. 다운로드에 사용할 네트워크 포트로 e0M을 선택합니다.
6. 지금 재부팅하려면 y를 입력하십시오.
7. 각 위치에 e0M의 IP 주소, 넷마스크 및 기본 게이트웨이를 입력합니다.

   ```
   <<var_nodeA_mgmt_ip>> <<var_nodeA_mgmt_mask>> <<var_nodeA_mgmt_gateway>>
   ```

8. 소프트웨어를 찾을 수 있는 URL을 입력합니다.

   ⓘ 이 웹 서버는 Ping할 수 있어야 합니다.

   ```
   <<var_url_boot_software>>
   ```

9. 사용자 이름에 대해 Enter 키를 눌러 사용자 이름이 없음을 나타냅니다.
10. 새로 설치한 소프트웨어를 이후 재부팅에 사용할 기본값으로 설정하려면 y 를 입력합니다.

11. y를 입력하여 노드를 재부팅합니다.

> 새 소프트웨어를 설치할 때 시스템이 BIOS 및 어댑터 카드에 대한 펌웨어 업그레이드를 수행할 수 있으며, 이로 인해 LOADER-A 프롬프트에서 재부팅되고 중지될 수 있습니다. 이러한 작업이 발생하면 시스템이 이 절차를 벗어날 수 있습니다.

12. Ctrl-C를 눌러 부팅 메뉴로 들어갑니다.
13. Clean Configuration(구성 정리) 및 Initialize All Disks(모든 디스크 초기화) 에 대해 옵션 4 를 선택합니다.
14. 디스크를 제로화하려면 y를 입력하고 구성을 재설정한 다음 새 파일 시스템을 설치합니다.
15. y 를 입력하여 디스크의 모든 데이터를 지웁니다.

> 연결된 디스크의 수와 유형에 따라 루트 애그리게이트의 초기화 및 생성을 완료하는 데 90분 이상이 걸릴 수 있습니다. 초기화가 완료되면 스토리지 시스템이 재부팅됩니다. SSD를 초기화하는 데 걸리는 시간은 상당히 줄어듭니다. 노드 A용 디스크가 제로화하는 동안 노드 B 구성을 계속할 수 있습니다.

노드 A를 초기화하는 동안 노드 B를 구성합니다

노드 **B**를 구성합니다

노드 B를 구성하려면 다음 단계를 완료하십시오.

1. 스토리지 시스템 콘솔 포트에 연결합니다. Loader-A 메시지가 표시됩니다. 하지만 스토리지 시스템이 재부팅 루프 상태인 경우 다음 메시지가 표시될 때 Ctrl-C를 눌러 자동 부팅 루프를 종료합니다.

```
Starting AUTOBOOT press Ctrl-C to abort…
```

2. Ctrl-C를 눌러 부팅 메뉴로 들어갑니다.

```
autoboot
```

3. 메시지가 나타나면 Ctrl-C를 누릅니다.

> ONTAP 9.6이 부팅 중인 소프트웨어 버전이 아닌 경우 다음 단계를 계속하여 새 소프트웨어를 설치하십시오. ONTAP 9.6이 부팅 중인 버전인 경우 옵션 8 및 y를 선택하여 노드를 재부팅합니다. 그런 다음 14단계를 계속합니다.

4. 새 소프트웨어를 설치하려면 옵션 7.A를 선택합니다
5. 업그레이드를 수행하려면 y 를 입력합니다.
6. 다운로드에 사용할 네트워크 포트로 e0M을 선택합니다.
7. 지금 재부팅하려면 y를 입력하십시오.
8. 각 위치에 e0M의 IP 주소, 넷마스크 및 기본 게이트웨이를 입력합니다.

```
<<var_nodeB_mgmt_ip>> <<var_nodeB_mgmt_ip>><<var_nodeB_mgmt_gateway>>
```

9. 소프트웨어를 찾을 수 있는 URL을 입력합니다.

   이 웹 서버는 Ping할 수 있어야 합니다.

```
<<var_url_boot_software>>
```

10. 사용자 이름에 대해 Enter 키를 눌러 사용자 이름이 없음을 나타냅니다.
11. 새로 설치한 소프트웨어를 이후 재부팅에 사용할 기본값으로 설정하려면 y 를 입력합니다.
12. y를 입력하여 노드를 재부팅합니다.

    새 소프트웨어를 설치할 때 시스템이 BIOS 및 어댑터 카드에 대한 펌웨어 업그레이드를 수행할 수 있으며, 이로 인해 LOADER-A 프롬프트에서 재부팅되고 중지될 수 있습니다. 이러한 작업이 발생하면 시스템이 이 절차를 벗어날 수 있습니다.

13. Ctrl-C를 눌러 부팅 메뉴로 들어갑니다.
14. Clean Configuration(구성 정리) 및 Initialize All Disks(모든 디스크 초기화) 에 대해 옵션 4 를 선택합니다.
15. 디스크를 제로화하려면 y를 입력하고 구성을 재설정한 다음 새 파일 시스템을 설치합니다.
16. y 를 입력하여 디스크의 모든 데이터를 지웁니다.

    연결된 디스크의 수와 유형에 따라 루트 애그리게이트의 초기화 및 생성을 완료하는 데 90분 이상이 걸릴 수 있습니다. 초기화가 완료되면 스토리지 시스템이 재부팅됩니다. SSD를 초기화하는 데 걸리는 시간은 상당히 줄어듭니다.

노드 **A** 구성 및 클러스터 구성 계속

스토리지 컨트롤러 A(노드 A) 콘솔 포트에 연결된 콘솔 포트 프로그램에서 노드 설정 스크립트를 실행합니다. 이 스크립트는 ONTAP 9.6이 처음으로 노드에서 부팅될 때 나타납니다.

ONTAP 9.6에서 노드 및 클러스터 설정 절차가 약간 변경되었습니다. 이제 클러스터 설정 마법사를 사용하여 클러스터의 첫 번째 노드를 구성하고 NetApp ONTAP System Manager(이전의 OnCommand ® System Manager)를 사용하여 클러스터를 구성할 수 있습니다.

1. 프롬프트에 따라 노드 A를 설정합니다

```
Welcome to the cluster setup wizard.
You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the cluster setup wizard.
     Any changes you made before quitting will be saved.
You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value.
This system will send event messages and periodic reports to NetApp
Technical
Support. To disable this feature, enter
autosupport modify -support disable
within 24 hours.
Enabling AutoSupport can significantly speed problem determination and
resolution should a problem occur on your system.
For further information on AutoSupport, see:
http://support.netapp.com/autosupport/
Type yes to confirm and continue {yes}: yes
Enter the node management interface port [e0M]:
Enter the node management interface IP address: <<var_nodeA_mgmt_ip>>
Enter the node management interface netmask: <<var_nodeA_mgmt_mask>>
Enter the node management interface default gateway:
<<var_nodeA_mgmt_gateway>>
A node management interface on port e0M with IP address
<<var_nodeA_mgmt_ip>> has been created.
Use your web browser to complete cluster setup by accessing
https://<<var_nodeA_mgmt_ip>>
Otherwise, press Enter to complete cluster setup using the command line
interface:
```

2. 노드의 관리 인터페이스의 IP 주소로 이동합니다.

> CLI를 사용하여 클러스터를 설정할 수도 있습니다. 이 문서에서는 System Manager의 설정에 따라 클러스터 설정에 대해 설명합니다.

3. Guided Setup(안내식 설정) 을 클릭하여 클러스터를 구성합니다.
4. 클러스터 이름은 <<var_clustername>>'을, 구성 중인 각 노드에 대해서는 <<var_NodeA>>'와 <<var_NodeB>>를 입력합니다. 스토리지 시스템에 사용할 암호를 입력합니다. 클러스터 유형으로 Switchless Cluster를 선택합니다. 클러스터 기본 라이센스를 입력합니다.
5. 클러스터, NFS 및 iSCSI에 대한 기능 라이센스도 입력할 수 있습니다.
6. 클러스터를 생성 중임을 나타내는 상태 메시지가 표시됩니다. 이 상태 메시지는 여러 상태를 순환합니다. 이 과정은 몇 분 정도 소요됩니다.
7. 네트워크를 구성합니다.
   a. IP 주소 범위 옵션을 선택 취소합니다.

b. Cluster Management IP Address 필드(<<var_clustermgmt_ip>>)에 넷마스크 필드(<<var_clustermgmt_mask>>)에 <<var_clustermgmt_gateway>>)를 입력합니다. 다음을 사용하십시오. 포트 필드의 선택기로 노드 A의 e0M을 선택합니다

c. 노드 A의 노드 관리 IP가 이미 채워져 있습니다. 노드 B에 대해 '<<var_NodeA_mgmt_ip>>'를 입력합니다

d. DNS Domain Name 필드에 '<<var_domain_name>>'을 입력합니다. DNS 서버 IP 주소 필드에 '<<var_dns_server_ip>>'를 입력합니다.

여러 DNS 서버 IP 주소를 입력할 수 있습니다.

e. Primary NTP Server 필드에 10.63.172.162 를 입력한다.

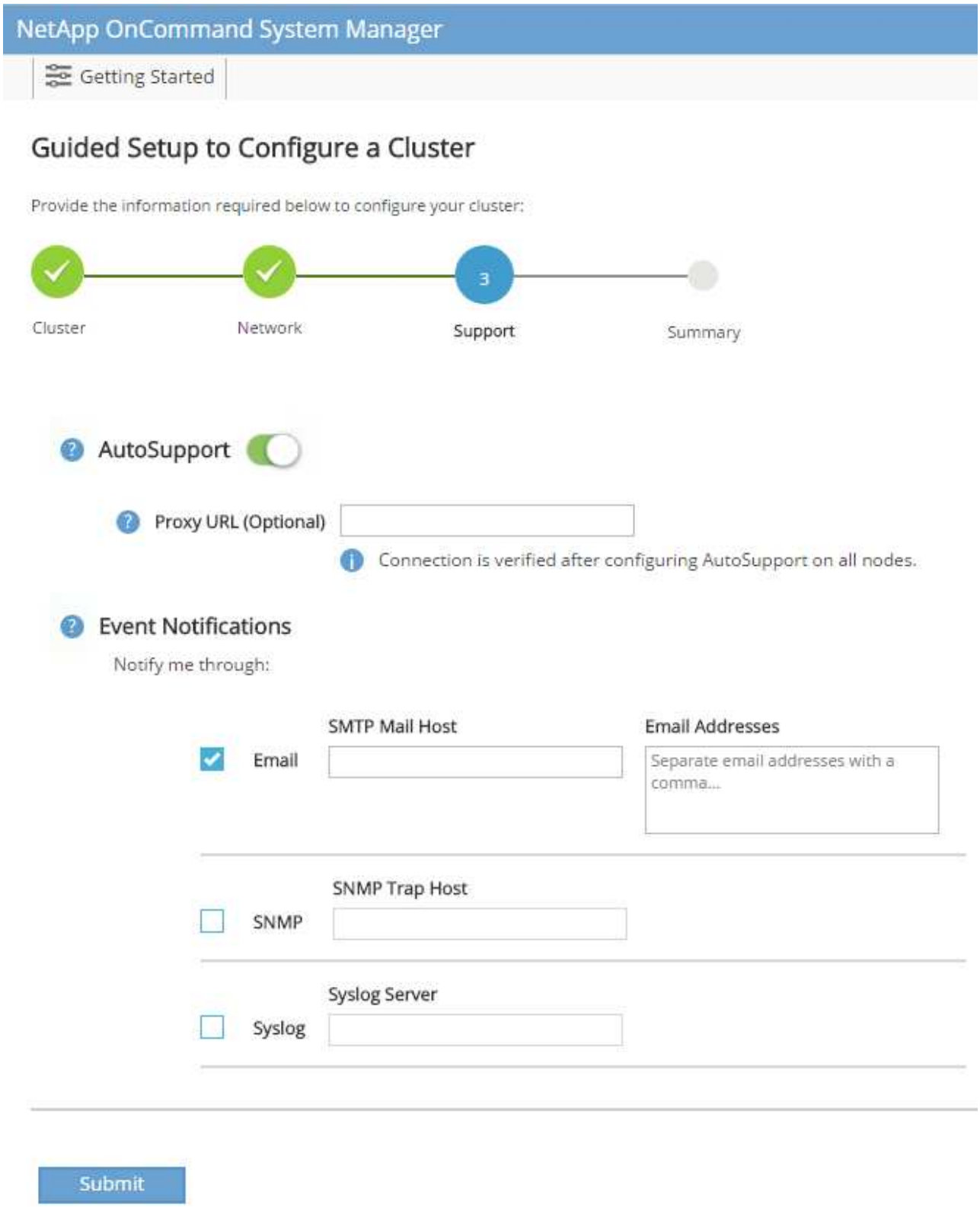
대체 NTP 서버를 입력할 수도 있습니다. '<<var_ntp_server_ip>>'의 IP 주소 '10.63.172.162'는 Nexus Mgmt IP입니다.

8. 지원 정보를 구성합니다.

a. 환경에 AutoSupport에 액세스하기 위한 프록시가 필요한 경우 프록시 URL에 URL을 입력합니다.

b. 이벤트 알림에 대한 SMTP 메일 호스트 및 이메일 주소를 입력합니다.

계속하려면 이벤트 알림 방법을 설정해야 합니다. 방법 중 하나를 선택할 수 있습니다.



시스템에서 클러스터 구성이 완료되었다는 메시지가 표시되면 클러스터 관리 를 클릭하여 스토리지를 구성합니다.

스토리지 클러스터 구성 계속

스토리지 노드 및 기본 클러스터를 구성한 후에는 스토리지 클러스터 구성을 계속할 수 있습니다.

모든 스페어 디스크를 제로합니다

클러스터의 모든 스페어 디스크를 제로하려면 다음 명령을 실행합니다.

```
disk zerospares
```

온보드 **UTA2** 포트 속성을 설정합니다

1. ucadmin show 명령을 실행하여 포트의 현재 모드 및 현재 유형을 확인합니다.

```
AFF C190::> ucadmin show
                     Current  Current    Pending  Pending    Admin
Node          Adapter  Mode     Type       Mode     Type       Status
------------  -------  -------  ---------  -------  ---------
-----------
AFF C190_A     0c       cna       target     -        -          online
AFF C190_A     0d       cna       target     -        -          online
AFF C190_A     0e       cna       target     -        -          online
AFF C190_A     0f       cna       target     -        -          online
AFF C190_B     0c       cna       target     -        -          online
AFF C190_B     0d       cna       target     -        -          online
AFF C190_B     0e       cna       target     -        -          online
AFF C190_B     0f       cna       target     -        -          online
8 entries were displayed.
```

2. 사용 중인 포트의 현재 모드가 CNA인지, 그리고 현재 유형이 타겟으로 설정되어 있는지 확인합니다. 그렇지 않은 경우 다음 명령을 사용하여 포트 속성을 변경합니다.

```
ucadmin modify -node <home node of the port> -adapter <port name> -mode
cna -type target
```

이전 명령을 실행하려면 포트가 오프라인 상태여야 합니다. 포트를 오프라인으로 전환하려면 다음 명령을 실행합니다.

```
network fcp adapter modify -node <home node of the port> -adapter <port
name> -state down
```

포트 속성을 변경한 경우 변경 사항을 적용하려면 각 노드를 재부팅해야 합니다.

관리 논리 인터페이스의 이름을 바꿉니다

관리 논리 인터페이스(LIF)의 이름을 변경하려면 다음 단계를 수행하십시오.

1. 현재 관리 LIF 이름을 표시합니다.

```
network interface show -vserver <<clustername>>
```

2. 클러스터 관리 LIF의 이름을 바꿉니다.

```
network interface rename -vserver <<clustername>> -lif
cluster_setup_cluster_mgmt_lif_1 -newname cluster_mgmt
```

3. 노드 B 관리 LIF의 이름을 바꿉니다.

```
network interface rename -vserver <<clustername>> -lif
cluster_setup_node_mgmt_lif_AFF C190_B_1 -newname AFF C190-02_mgmt1
```

클러스터 관리에서 자동 되돌리기 설정

클러스터 관리 인터페이스에서 자동 되돌리기 매개 변수를 설정합니다.

```
network interface modify -vserver <<clustername>> -lif cluster_mgmt -auto-
revert true
```

서비스 프로세서 네트워크 인터페이스를 설정합니다

각 노드의 서비스 프로세서에 정적 IPv4 주소를 할당하려면 다음 명령을 실행합니다.

```
system service-processor network modify -node <<var_nodeA>> -address
-family IPv4 -enable true -dhcp none -ip-address <<var_nodeA_sp_ip>>
-netmask <<var_nodeA_sp_mask>> -gateway <<var_nodeA_sp_gateway>>
system service-processor network modify -node <<var_nodeB>> -address
-family IPv4 -enable true -dhcp none -ip-address <<var_nodeB_sp_ip>>
-netmask <<var_nodeB_sp_mask>> -gateway <<var_nodeB_sp_gateway>>
```

서비스 프로세서 IP 주소는 노드 관리 IP 주소와 동일한 서브넷에 있어야 합니다.

ONTAP에서 스토리지 페일오버 설정

스토리지 페일오버가 설정되었는지 확인하려면 페일오버 쌍에서 다음 명령을 실행합니다.

1. 스토리지 페일오버 상태를 확인합니다.

```
storage failover show
```

'<<var_NodeA>>'와 '<<var_NodeB>>'는 모두 테이크오버를 수행할 수 있어야 합니다. 노드가 테이크오버 수행 가능한 경우 3단계로 이동하십시오.

2. 두 노드 중 하나에서 페일오버가 사용되도록 설정합니다.

```
storage failover modify -node <<var_nodeA>> -enabled true
```

한 노드에서 페일오버가 사용되도록 설정하면 두 노드 모두에서 설정됩니다.

3. 2노드 클러스터의 HA 상태를 확인합니다.

2개 이상의 노드가 있는 클러스터에는 이 단계를 적용할 수 없습니다.

```
cluster ha show
```

4. 고가용성이 구성된 경우 6단계로 이동합니다. 고가용성이 구성된 경우 명령을 실행하면 다음 메시지가 표시됩니다.

```
High Availability Configured: true
```

5. 2노드 클러스터에만 HA 모드를 사용하도록 설정합니다.

2개 이상의 노드가 있는 클러스터에서는 페일오버에 문제가 발생하므로 이 명령을 실행하지 마십시오.

```
cluster ha modify -configured true
Do you want to continue? {y|n}: y
```

6. 하드웨어 지원이 올바르게 구성되어 있는지 확인하고 필요한 경우 파트너 IP 주소를 수정합니다.

```
storage failover hwassist show
```

"Keep Alive Status: Error:" 메시지는 컨트롤러 중 하나가 파트너의 hwassist keep alive 경고를 받지 못했음을 나타내며, 이는 하드웨어 지원이 구성되지 않았음을 나타냅니다. 다음 명령을 실행하여 하드웨어 지원을 구성합니다.

```
storage failover modify –hwassist-partner-ip <<var_nodeB_mgmt_ip>> -node
<<var_nodeA>>
storage failover modify –hwassist-partner-ip <<var_nodeA_mgmt_ip>> -node
<<var_nodeB>>
```

ONTAP에서 점보 프레임 MTU 브로드캐스트 도메인을 생성합니다

MTU가 9000인 데이터 브로드캐스트 도메인을 생성하려면 다음 명령을 실행합니다.

```
broadcast-domain create -broadcast-domain Infra_NFS -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-A -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-B -mtu 9000
```

기본 브로드캐스트 도메인에서 데이터 포트를 제거합니다

10GbE 데이터 포트는 iSCSI/NFS 트래픽에 사용되며 이러한 포트는 기본 도메인에서 제거해야 합니다. 포트 e0e 및 e0f는 사용되지 않으며 기본 도메인에서도 제거해야 합니다.

브로드캐스트 도메인에서 포트를 제거하려면 다음 명령을 실행합니다.

```
broadcast-domain remove-ports -broadcast-domain Default -ports
<<var_nodeA>>:e0c, <<var_nodeA>>:e0d, <<var_nodeA>>:e0e,
<<var_nodeA>>:e0f, <<var_nodeB>>:e0c, <<var_nodeB>>:e0d,
<<var_nodeA>>:e0e, <<var_nodeA>>:e0f
```

UTA2 포트에서 흐름 제어를 사용하지 않도록 설정합니다

외부 장치에 연결된 모든 UTA2 포트에서 흐름 제어를 사용하지 않도록 설정하는 것이 NetApp의 모범 사례입니다. 흐름 제어를 사용하지 않도록 설정하려면 다음 명령을 실행합니다.

```
net port modify -node <<var_nodeA>> -port e0c -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0d -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0e -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0f -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0c -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0d -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0e -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0f -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
```

ONTAP에서 인터페이스 그룹 **LACP**를 구성합니다

이 인터페이스 그룹 유형에 2개 이상의 이더넷 인터페이스와 LACP를 지원하는 스위치가 필요합니다. 섹션 5.1의 이 가이드에 설명된 단계를 기준으로 구성되었는지 확인합니다.

클러스터 프롬프트에서 다음 단계를 완료합니다.

```
ifgrp create -node <<var_nodeA>> -ifgrp a0a -distr-func port -mode
multimode_lacp
network port ifgrp add-port -node <<var_nodeA>> -ifgrp a0a -port e0c
network port ifgrp add-port -node <<var_nodeA>> -ifgrp a0a -port e0d
ifgrp create -node << var_nodeB>> -ifgrp a0a -distr-func port -mode
multimode_lacp
network port ifgrp add-port -node <<var_nodeB>> -ifgrp a0a -port e0c
network port ifgrp add-port -node <<var_nodeB>> -ifgrp a0a -port e0d
```

ONTAP에서 점보 프레임을 구성합니다

점보 프레임(일반적으로 9,000바이트 MTU 사용)을 사용하도록 ONTAP 네트워크 포트를 구성하려면 클러스터 쉘에서 다음 명령을 실행합니다.

```
AFF C190::> network port modify -node node_A -port a0a -mtu 9000
Warning: This command will cause a several second interruption of service
on
         this network port.
Do you want to continue? {y|n}: y
AFF C190::> network port modify -node node_B -port a0a -mtu 9000
Warning: This command will cause a several second interruption of service
on
         this network port.
Do you want to continue? {y|n}: y
```

ONTAP에서 VLAN을 생성합니다

ONTAP에서 VLAN을 생성하려면 다음 단계를 수행하십시오.

1. NFS VLAN 포트를 생성하여 데이터 브로드캐스트 도메인에 추가합니다.

```
network port vlan create –node <<var_nodeA>> -vlan-name a0a-
<<var_nfs_vlan_id>>
network port vlan create –node <<var_nodeB>> -vlan-name a0a-
<<var_nfs_vlan_id>>
broadcast-domain add-ports -broadcast-domain Infra_NFS -ports
<<var_nodeA>>:a0a-<<var_nfs_vlan_id>>, <<var_nodeB>>:a0a-
<<var_nfs_vlan_id>>
```

2. iSCSI VLAN 포트를 생성하여 데이터 브로드캐스트 도메인에 추가합니다.

```
network port vlan create –node <<var_nodeA>> -vlan-name a0a-
<<var_iscsi_vlan_A_id>>
network port vlan create –node <<var_nodeA>> -vlan-name a0a-
<<var_iscsi_vlan_B_id>>
network port vlan create –node <<var_nodeB>> -vlan-name a0a-
<<var_iscsi_vlan_A_id>>
network port vlan create –node <<var_nodeB>> -vlan-name a0a-
<<var_iscsi_vlan_B_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-A -ports
<<var_nodeA>>:a0a-<<var_iscsi_vlan_A_id>>,<<var_nodeB>>:a0a-
<<var_iscsi_vlan_A_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-B -ports
<<var_nodeA>>:a0a-<<var_iscsi_vlan_B_id>>,<<var_nodeB>>:a0a-
<<var_iscsi_vlan_B_id>>
```

3. MGMT-VLAN 포트를 생성합니다.

```
network port vlan create –node <<var_nodeA>> -vlan-name a0a-
<<mgmt_vlan_id>>
network port vlan create –node <<var_nodeB>> -vlan-name a0a-
<<mgmt_vlan_id>>
```

ONTAP에서 데이터 애그리게이트를 생성합니다

ONTAP 설정 프로세스 중에 루트 볼륨이 포함된 애그리게이트가 생성됩니다. 추가 애그리게이트를 생성하려면 애그리게이트 이름, 애그리게이트를 생성할 노드, 애그리게이트에 포함된 디스크 수를 결정합니다.

Aggregate를 생성하려면 다음 명령을 실행합니다.

```
aggr create -aggregate aggr1_nodeA -node <<var_nodeA>> -diskcount
<<var_num_disks>>
aggr create -aggregate aggr1_nodeB -node <<var_nodeB>> -diskcount
<<var_num_disks>>
```

구성에 최소 하나의 디스크(가장 큰 디스크 선택)를 스페어로 보관합니다. 모범 사례는 각 디스크 유형 및 크기에 대해 하나 이상의 스페어를 두는 것입니다.

5개의 디스크로 시작합니다. 스토리지를 추가해야 할 때 디스크를 애그리게이트에 추가할 수 있습니다.

디스크 비우기가 완료될 때까지 애그리게이트를 생성할 수 없습니다. 집계 생성 상태를 표시하려면 'aggr show' 명령을 실행합니다. aggr1_NodeA가 온라인 상태가 될 때까지 진행하지 마십시오.

ONTAP에서 표준 시간대를 구성합니다

시간 동기화를 구성하고 클러스터에서 표준 시간대를 설정하려면 다음 명령을 실행합니다.

```
timezone <<var_timezone>>
```

예를 들어 미국 동부의 표준 시간대는 America/New_York입니다. 표준 시간대 이름을 입력하기 시작하면 Tab 키를 눌러 사용 가능한 옵션을 확인합니다.

ONTAP에서 SNMP를 구성합니다

SNMP를 구성하려면 다음 단계를 수행하십시오.

1. 위치 및 연락처와 같은 SNMP 기본 정보를 구성합니다. 이 정보는 SNMP에서 'SysLocation', 'SysContact' 변수로 표시됩니다.

```
snmp contact <<var_snmp_contact>>
snmp location "<<var_snmp_location>>"
snmp init 1
options snmp.enable on
```

2. 원격 호스트에 보낼 SNMP 트랩을 구성합니다.

```
snmp traphost add <<var_snmp_server_fqdn>>
```

ONTAP에서 SNMPv1을 구성합니다

SNMPv1을 구성하려면 커뮤니티라는 공유 암호 일반 텍스트 암호를 설정합니다.

```
snmp community add ro <<var_snmp_community>>
```

NMP community delete all 명령을 주의하여 사용한다. 다른 모니터링 제품에 커뮤니티 문자열을 사용하는 경우 이 명령은 해당 문자열을 제거합니다.

ONTAP에서 SNMPv3을 구성합니다

SNMPv3을 사용하려면 인증을 위해 사용자를 정의하고 구성해야 합니다. SNMPv3을 구성하려면 다음 단계를 수행하십시오.

1. Security snmpusers 명령을 실행하여 엔진 ID를 조회한다.
2. 'snmpv3user'라는 사용자를 생성합니다.

```
security login create -username snmpv3user -authmethod usm -application
snmp
```

3. 권한 있는 엔터티의 엔진 ID를 입력하고 인증 프로토콜로 md5를 선택합니다.
4. 메시지가 나타나면 인증 프로토콜에 사용할 최소 길이 8자로 된 암호를 입력합니다.
5. 개인 정보 보호 프로토콜로 des 를 선택합니다.
6. 메시지가 나타나면 개인 정보 보호 프로토콜에 사용할 최소 길이 8자로 된 암호를 입력합니다.

ONTAP에서 **AutoSupport HTTPS**를 구성합니다

NetApp AutoSupport 툴은 HTTPS를 통해 지원 요약 정보를 NetApp에 보냅니다. AutoSupport를 구성하려면 다음 명령을 실행합니다.

```
system node autosupport modify -node * -state enable –mail-hosts
<<var_mailhost>> -transport https -support enable -noteto
<<var_storage_admin_email>>
```

스토리지 가상 머신을 생성합니다

인프라 스토리지 가상 시스템(SVM)을 생성하려면 다음 단계를 완료하십시오.

1. 'vserver create' 명령을 실행합니다.

```
vserver create –vserver Infra-SVM –rootvolume rootvol –aggregate
aggr1_nodeA –rootvolume-security-style unix
```

2. NetApp VSC를 위한 인프라-SVM 애그리게이트 목록에 데이터 애그리게이트를 추가합니다.

```
vserver modify -vserver Infra-SVM -aggr-list aggr1_nodeA,aggr1_nodeB
```

3. NFS와 iSCSI를 남겨두고 SVM에서 사용하지 않는 스토리지 프로토콜을 제거합니다.

```
vserver remove-protocols –vserver Infra-SVM -protocols cifs,ndmp,fcp
```

4. 인프라 SVM에서 NFS 프로토콜을 사용하고 실행합니다.

```
nfs create -vserver Infra-SVM -udp disabled
```

5. NetApp NFS VAAI 플러그인에 대한 'VM vStorage' 매개 변수를 설정합니다. 그런 다음 NFS가 구성되었는지 확인합니다.

```
vserver nfs modify –vserver Infra-SVM –vstorage enabled
vserver nfs show
```

SVM은 이전에 SVM을 vserver라고 했기 때문에 명령줄에서는 "vserver"가 명령을 앞에 표시합니다.

ONTAP에서 NFSv3을 구성합니다

다음 표에는 이 구성을 완료하는 데 필요한 정보가 나와 있습니다.

세부 정보	상세 값
ESXi 호스트 NFS IP 주소입니다	<<var_esxi_hostA_nfs_ip>> 를 참조하십시오
ESXi 호스트 B NFS IP 주소입니다	<<var_esxi_hostB_nfs_ip>> 를 참조하십시오

SVM에서 NFS를 구성하려면 다음 명령을 실행합니다.

1. 기본 엑스포트 정책에서 각 ESXi 호스트에 대한 규칙을 생성합니다.
2. 생성 중인 각 ESXi 호스트에 대해 규칙을 할당합니다. 각 호스트에는 고유한 규칙 인덱스가 있습니다. 첫 번째 ESXi 호스트에는 규칙 인덱스 1이 있고 두 번째 ESXi 호스트에는 규칙 인덱스 2가 있습니다.

```
vserver export-policy rule create –vserver Infra-SVM -policyname default
–ruleindex 1 –protocol nfs -clientmatch <<var_esxi_hostA_nfs_ip>>
-rorule sys –rwrule sys -superuser sys –allow-suid false
vserver export-policy rule create –vserver Infra-SVM -policyname default
–ruleindex 2 –protocol nfs -clientmatch <<var_esxi_hostB_nfs_ip>>
-rorule sys –rwrule sys -superuser sys –allow-suid false
vserver export-policy rule show
```

3. 인프라 SVM 루트 볼륨에 엑스포트 정책을 할당합니다.

```
volume modify –vserver Infra-SVM –volume rootvol –policy default
```

vSphere를 설정한 후 NetApp VSC는 엑스포트 정책을 자동으로 처리합니다. 설치하지 않은 경우 Cisco UCS C-Series 서버를 추가할 때 엑스포트 정책 규칙을 생성해야 합니다.

ONTAP에서 iSCSI 서비스를 생성합니다

SVM에서 iSCSI 서비스를 생성하려면 다음 명령을 실행합니다. 또한 이 명령은 iSCSI 서비스를 시작하고 SVM에 대한 iSCSI IQN을 설정합니다. iSCSI가 구성되었는지 확인합니다.

```
iscsi create -vserver Infra-SVM
iscsi show
```

ONTAP에서 SVM 루트 볼륨의 로드 공유 미러를 생성합니다

ONTAP에서 SVM 루트 볼륨의 로드 공유 미러를 생성하려면 다음 단계를 수행하십시오.

1. 각 노드에서 인프라 SVM 루트 볼륨의 로드 공유 미러가 될 볼륨을 생성합니다.

```
volume create –vserver Infra_Vserver –volume rootvol_m01 –aggregate
aggr1_nodeA –size 1GB –type DP
volume create –vserver Infra_Vserver –volume rootvol_m02 –aggregate
aggr1_nodeB –size 1GB –type DP
```

2. 15분마다 루트 볼륨 미러 관계를 업데이트하는 작업 스케줄을 생성합니다.

```
job schedule interval create -name 15min -minutes 15
```

3. 미러링 관계를 생성합니다.

```
snapmirror create -source-path Infra-SVM:rootvol -destination-path
Infra-SVM:rootvol_m01 -type LS -schedule 15min
snapmirror create -source-path Infra-SVM:rootvol -destination-path
Infra-SVM:rootvol_m02 -type LS -schedule 15min
```

4. 미러링 관계를 초기화하고 미러링 관계가 만들어졌는지 확인합니다.

```
snapmirror initialize-ls-set -source-path Infra-SVM:rootvol
snapmirror show
```

ONTAP에서 HTTPS 액세스를 구성합니다

스토리지 컨트롤러에 대한 보안 액세스를 구성하려면 다음 단계를 수행하십시오.

1. 인증서 명령에 액세스할 수 있도록 권한 수준을 높입니다.

```
set -privilege diag
Do you want to continue? {y|n}: y
```

2. 일반적으로 자체 서명된 인증서가 이미 있습니다. 다음 명령을 실행하여 인증서를 확인합니다.

```
security certificate show
```

3. 표시된 각 SVM에서 인증서 공통 이름은 SVM의 DNS FQDN과 일치해야 합니다. 네 개의 기본 인증서를 삭제하고 자체 서명된 인증서 또는 인증 기관의 인증서로 대체해야 합니다.

> 인증서를 만들기 전에 만료된 인증서를 삭제하는 것이 좋습니다. 만료된 인증서를 삭제하려면 보안 인증서 삭제 명령을 실행합니다. 다음 명령에서 Tab completion을 사용하여 각 기본 인증서를 선택하고 삭제합니다.

```
security certificate delete [TAB] …
Example: security certificate delete -vserver Infra-SVM -common-name
Infra-SVM -ca Infra-SVM -type server -serial 552429A6
```

4. 자체 서명된 인증서를 생성하고 설치하려면 다음 명령을 일회성 명령으로 실행합니다. 인프라 SVM 및 클러스터 SVM에 대한 서버 인증서를 생성합니다. 다시 한 번 탭 완료 기능을 사용하면 이러한 명령을 쉽게 완료할 수 있습니다.

```
security certificate create [TAB] …
Example: security certificate create -common-name infra-svm.netapp.com
-type server -size 2048 -country US -state "North Carolina" -locality
"RTP" -organization "NetApp" -unit "FlexPod" -email-addr
"abc@netapp.com" -expire-days 3650 -protocol SSL -hash-function SHA256
-vserver Infra-SVM
```

5. 다음 단계에 필요한 매개 변수의 값을 가져오려면 security certificate show 명령을 실행합니다.
6. '–server-enabled true' 및 '–client-enabled false' 매개 변수를 사용하여 방금 만든 각 인증서를 활성화합니다. 다시 탭 완료를 사용합니다.

```
security ssl modify [TAB] …
Example: security ssl modify -vserver Infra-SVM -server-enabled true
-client-enabled false -ca infra-svm.netapp.com -serial 55243646 -common
-name infra-svm.netapp.com
```

7. SSL 및 HTTPS 액세스를 구성 및 활성화하고 HTTP 액세스를 비활성화합니다.

```
system services web modify -external true -sslv3-enabled true
Warning: Modifying the cluster configuration will cause pending web
service requests to be interrupted as the web servers are restarted.
Do you want to continue {y|n}: y
system services firewall policy delete -policy mgmt -service http
–vserver <<var_clustername>>
```

명령 실행 중 일부에서 항목이 존재하지 않는다는 오류 메시지가 반환되는 것은 정상입니다.

8. 관리 권한 수준으로 되돌아가며 설치를 생성하여 SVM을 웹에서 사용할 수 있도록 합니다.

```
set -privilege admin
vserver services web modify -name spi -vserver * -enabled true
```

ONTAP에서 NetApp FlexVol 볼륨을 생성합니다

NetApp FlexVol ® 볼륨을 생성하려면 볼륨 이름, 크기 및 해당 볼륨을 입력합니다. 2개의 VMware 데이터 저장소 볼륨과 서버 부팅 볼륨을 생성합니다.

```
volume create -vserver Infra-SVM -volume infra_datastore -aggregate
aggr1_nodeB -size 500GB -state online -policy default -junction-path
/infra_datastore -space-guarantee none -percent-snapshot-space 0
volume create -vserver Infra-SVM -volume infra_swap -aggregate aggr1_nodeA
-size 100GB -state online -policy default -junction-path /infra_swap
-space-guarantee none -percent-snapshot-space 0 -snapshot-policy none
-efficiency-policy none
volume create -vserver Infra-SVM -volume esxi_boot -aggregate aggr1_nodeA
-size 100GB -state online -policy default -space-guarantee none -percent
-snapshot-space 0
```

ONTAP에서 LUN을 생성합니다

2개의 부팅 LUN을 생성하려면 다음 명령을 실행합니다.

```
lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-A -size
15GB -ostype vmware -space-reserve disabled
lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-B -size
15GB -ostype vmware -space-reserve disabled
```

Cisco UCS C-Series 서버를 더 추가할 때는 부팅 LUN을 더 생성해야 합니다.

ONTAP에서 iSCSI LIF를 생성합니다

다음 표에는 이 구성을 완료하는 데 필요한 정보가 나와 있습니다.

세부 정보	상세 값
스토리지 노드 A iSCSI LIF01A	<<var_NodeA_iscsi_lif01a_ip>> 를 참조하십시오
스토리지 노드 A iSCSI LIF01A 네트워크 마스크입니다	<<var_NodeA_iscsi_lif01a_mask>>
스토리지 노드 A iSCSI LIF01B	<<var_NodeA_iscsi_liff 01b_ip>> 를 참조하십시오

세부 정보	상세 값
스토리지 노드 A iSCSI LIF01B 네트워크 마스크입니다	<<var_NodeA_iscsi_liff 01b_mask>>
스토리지 노드 B iSCSI LIF01A	<<var_NodeB_iscsi_liff 01a_ip>>
스토리지 노드 B iSCSI LIF01A 네트워크 마스크입니다	<<var_NodeB_iscsi_liff 01a_mask>>
스토리지 노드 B iSCSI LIF01B	<<var_NodeB_iscsi_liff 01b_ip>>
스토리지 노드 B iSCSI LIF01B 네트워크 마스크입니다	<<var_NodeB_iscsi_liff 01b_mask>>

각 노드에 2개의 iSCSI LIF를 4개 생성합니다.

```
network interface create -vserver Infra-SVM -lif iscsi_lif01a -role data
-data-protocol iscsi -home-node <<var_nodeA>> -home-port a0a-
<<var_iscsi_vlan_A_id>> -address <<var_nodeA_iscsi_lif01a_ip>> -netmask
<<var_nodeA_iscsi_lif01a_mask>> –status-admin up –failover-policy disabled
–firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif01b -role data
-data-protocol iscsi -home-node <<var_nodeA>> -home-port a0a-
<<var_iscsi_vlan_B_id>> -address <<var_nodeA_iscsi_lif01b_ip>> -netmask
<<var_nodeA_iscsi_lif01b_mask>> –status-admin up –failover-policy disabled
–firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02a -role data
-data-protocol iscsi -home-node <<var_nodeB>> -home-port a0a-
<<var_iscsi_vlan_A_id>> -address <<var_nodeB_iscsi_lif01a_ip>> -netmask
<<var_nodeB_iscsi_lif01a_mask>> –status-admin up –failover-policy disabled
–firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02b -role data
-data-protocol iscsi -home-node <<var_nodeB>> -home-port a0a-
<<var_iscsi_vlan_B_id>> -address <<var_nodeB_iscsi_lif01b_ip>> -netmask
<<var_nodeB_iscsi_lif01b_mask>> –status-admin up –failover-policy disabled
–firewall-policy data –auto-revert false
network interface show
```

ONTAP에서 NFS LIF를 생성합니다

다음 표에는 이 구성을 완료하는 데 필요한 정보가 나와 있습니다.

세부 정보	상세 값
스토리지 노드 A NFS LIF 01 IP입니다	<<var_NodeA_nfs_lif_01_ip>>
스토리지 노드 A NFS LIF 01 네트워크 마스크	<<var_NodeA_nfs_lif_01_mask>>
스토리지 노드 B NFS LIF 02 IP	<<var_NodeB_nfs_lif_02_ip>>
스토리지 노드 B NFS LIF 02 네트워크 마스크	<<var_NodeB_nfs_lif_02_mask>>

NFS LIF를 생성합니다.

```
network interface create -vserver Infra-SVM -lif nfs_lif01 -role data
-data-protocol nfs -home-node <<var_nodeA>> -home-port a0a-
<<var_nfs_vlan_id>> -address <<var_nodeA_nfs_lif_01_ip>> -netmask <<
var_nodeA_nfs_lif_01_mask>> -status-admin up –failover-policy broadcast-
domain-wide –firewall-policy data –auto-revert true
network interface create -vserver Infra-SVM -lif nfs_lif02 -role data
-data-protocol nfs -home-node <<var_nodeA>> -home-port a0a-
<<var_nfs_vlan_id>> –address <<var_nodeB_nfs_lif_02_ip>> -netmask <<
var_nodeB_nfs_lif_02_mask>> -status-admin up –failover-policy broadcast-
domain-wide –firewall-policy data –auto-revert true
network interface show
```

인프라 **SVM** 관리자를 추가합니다

다음 표에는 SVM 관리자를 추가하는 데 필요한 정보가 나와 있습니다.

세부 정보	상세 값
Vsmgmt IP	<<var_svm_mgmt_ip>> 를 입력합니다
Vsmgmt 네트워크 마스크	<<var_svm_mgmt_mask>>
Vsmgmt 기본 게이트웨이	<<var_svm_mgmt_gateway>>

관리 네트워크에 인프라 SVM 관리자 및 SVM 관리 논리 인터페이스를 추가하려면 다음 단계를 완료하십시오.

1. 다음 명령을 실행합니다.

```
network interface create –vserver Infra-SVM –lif vsmgmt –role data
-data-protocol none –home-node <<var_nodeB>> -home-port  e0M –address
<<var_svm_mgmt_ip>> -netmask <<var_svm_mgmt_mask>> -status-admin up
–failover-policy broadcast-domain-wide –firewall-policy mgmt –auto-
revert true
```

> 여기서 SVM 관리 IP는 스토리지 클러스터 관리 IP와 동일한 서브넷에 있어야 합니다.

2. 기본 경로를 생성하여 SVM 관리 인터페이스가 외부 환경에 도달할 수 있도록 합니다.

```
network route create –vserver Infra-SVM -destination 0.0.0.0/0 –gateway
<<var_svm_mgmt_gateway>>
network route show
```

3. SVM vsadmin 사용자의 암호를 설정하고 사용자 잠금을 해제합니다.

```
security login password –username vsadmin –vserver Infra-SVM
Enter a new password: <<var_password>>
Enter it again: <<var_password>>
security login unlock –username vsadmin –vserver Infra-SVM
```

"다음으로 Cisco UCS C-Series 랙 서버를 구축합니다."

Cisco UCS C-Series 랙 서버 구축

이 섹션에서는 FlexPod Express 구성에 사용할 Cisco UCS C-Series 독립 실행형 랙 서버를 구성하기 위한 절차를 세부적으로 설명합니다.

CIMC에 대한 초기 **Cisco UCS C-Series** 독립 실행형 서버 설정을 수행합니다

Cisco UCS C-Series 독립 실행형 서버에 대한 CIMC 인터페이스의 초기 설정을 위해 다음 단계를 완료합니다.

다음 표에는 각 Cisco UCS C-Series 독립 실행형 서버에 대한 CIMC를 구성하는 데 필요한 정보가 나와 있습니다.

세부 정보	상세 값
CIMC IP 주소	CIMC_IP>\< CIMC_IP>>
CIMC 서브넷 마스크	CIMC_NETMASK
CIMC 기본 게이트웨이	CIMC_GATELOGATE>\<<CIMC_Gateway>

이 검증에 사용된 CIMC 버전은 CIMC 4.0입니다(4).

모든 서버

1. 서버와 함께 제공된 Cisco 키보드, 비디오 및 마우스(KVM) 동글을 서버 앞의 KVM 포트에 연결합니다. VGA 모니터와 USB 키보드의 플러그를 적절한 KVM 동글 포트에 꽂습니다.

   서버의 전원을 켜고 CIMC 구성을 시작할지 묻는 메시지가 표시되면 F8 키를 누릅니다.

2. CIMC 구성 유틸리티에서 다음 옵션을 설정합니다.

   a. 네트워크 인터페이스 카드(NIC) 모드:

      전용 '[X]'

   b. IP(기본):

      IPv4: '[X]'

      DHCP 활성화: "[]"

      CIMC IP:<<CIMC_IP>>'를 선택합니다

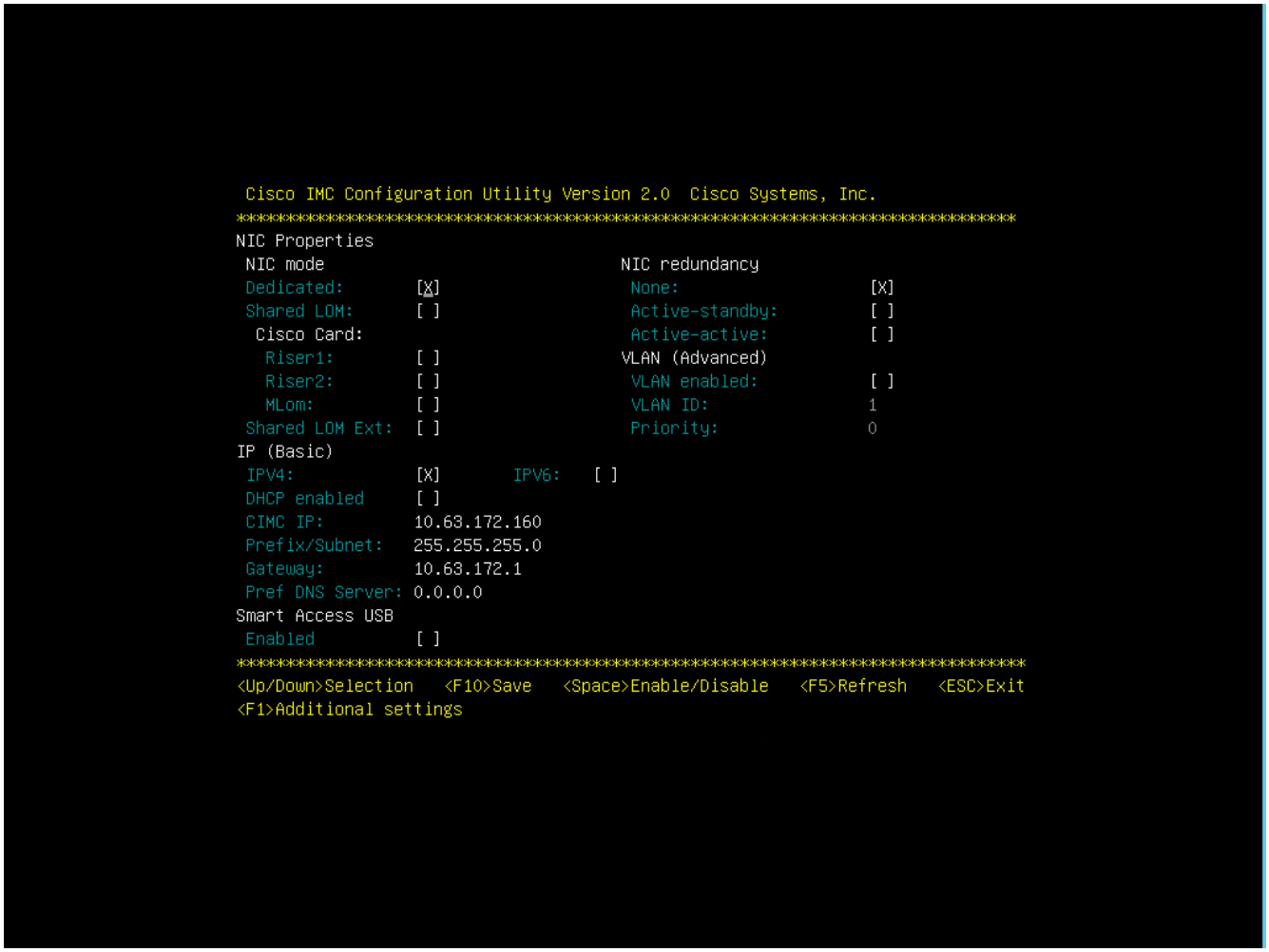
      Prefix/Subnet:<<CIMC_Netmask>>'입니다

      Gateway:<<CIMC_Gateway>>'입니다

   c. VLAN(고급): VLAN 태깅을 사용하지 않도록 설정하려면 선택되지 않은 상태로 둡니다.

      NIC 이중화

      없음: '[X]'



3. F1을 눌러 추가 설정을 확인합니다.

   a. 공통 속성:

      호스트 이름: "\< ESXi_host_name>>"

      동적 DNS: "[]"

      공장 출하시 기본값: 선택하지 않은 상태로 둡니다.

   b. 기본 사용자(기본):

      기본 암호: "<<admin_password>>"

      '\<<admin_password>' 암호를 다시 입력하십시오

      포트 속성: 기본값을 사용합니다.

   포트 프로파일: 선택하지 않은 상태로 둡니다.

4. F10 키를 눌러 CIMC 인터페이스 구성을 저장합니다.
5. 구성을 저장한 후 Esc 키를 눌러 종료합니다.

Cisco UCS C-Series 서버 iSCSI 부트를 구성합니다

이 FlexPod Express 구성에서 VIC1457은 iSCSI 부팅에 사용됩니다.

다음 표에는 iSCSI 부트를 구성하는 데 필요한 정보가 나와 있습니다.

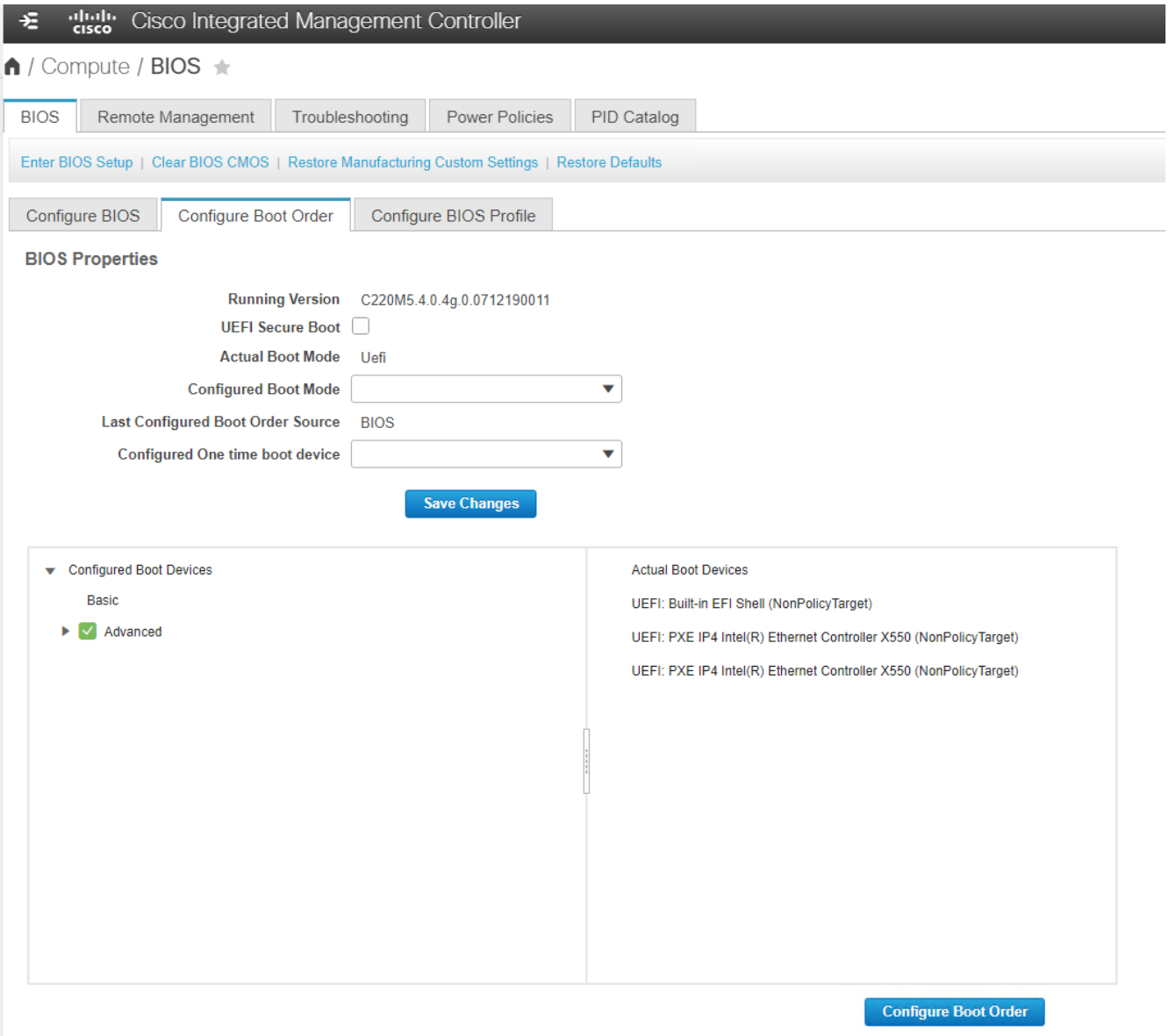
기울임꼴로 표시된 글꼴은 각 ESXi 호스트에 대해 고유한 변수를 나타냅니다.

세부 정보	상세 값
ESXi 호스트 이니시에이터에서 이름을 입력합니다	<<var_UCS_initiator_name_a>>
ESXi 호스트 iSCSI - A IP	<<var_esxi_host_iscsiA_ip>>
ESXi 호스트 iSCSI - 네트워크 마스크입니다	<<var_esxi_host_iscsiA_mask>>
ESXi 호스트 iSCSI 기본 게이트웨이입니다	<<var_esxi_host_iscsiA_gateway>>
ESXi 호스트 이니시에이터 B 이름입니다	<<var_UCS_initiator_name_B>>
ESXi 호스트 iSCSI-B IP	<<var_esxi_host_iscsiB_ip>>
ESXi 호스트 iSCSI-B 네트워크 마스크	<<var_esxi_host_iscsiB_mask>>
ESXi 호스트 iSCSI-B 게이트웨이	<<var_esxi_host_iscsiB_gateway>>
IP 주소 iscsi_liff 01a	<<var_iscsi_liff 01a>>
IP 주소 iscsi_lif02a	<<var_iscsi_lif02a>> 를 참조하십시오
IP 주소 iscsi_liff 01b	<<var_iscsi_liff 01b>>
IP 주소 iscsi_liff 02b	<<var_iscsi_liff 02b>> 를 참조하십시오
infra_SVM IQN을 선택합니다	<<var_SVM_IQN>>을 참조하십시오

부팅 순서 구성

부팅 순서 구성을 설정하려면 다음 단계를 수행하십시오.

1. CIMC 인터페이스 브라우저 창에서 Compute 탭을 클릭하고 BIOS를 선택합니다.
2. Configure Boot Order(부팅 순서 구성) 를 클릭한 다음 OK(확인) 를 클릭합니다.



3. Add Boot Device(부팅 장치 추가) 에서 장치를 클릭하고 Advanced(고급) 탭으로 이동하여 다음 장치를 구성합니다.

   a. 가상 미디어 추가:

      이름: kvm-cd-dvd

      하위 유형: KVM 매핑된 DVD

      상태: 활성화됨

      순서: 1

   b. iSCSI 부팅 추가:

      이름: iscsi-a

      상태: 활성화됨

주문: 2

슬롯: mLOM

포트: 1

c. Add iSCSI Boot(iSCSI 부팅 추가) 를 클릭합니다.

이름: iSCSI-B

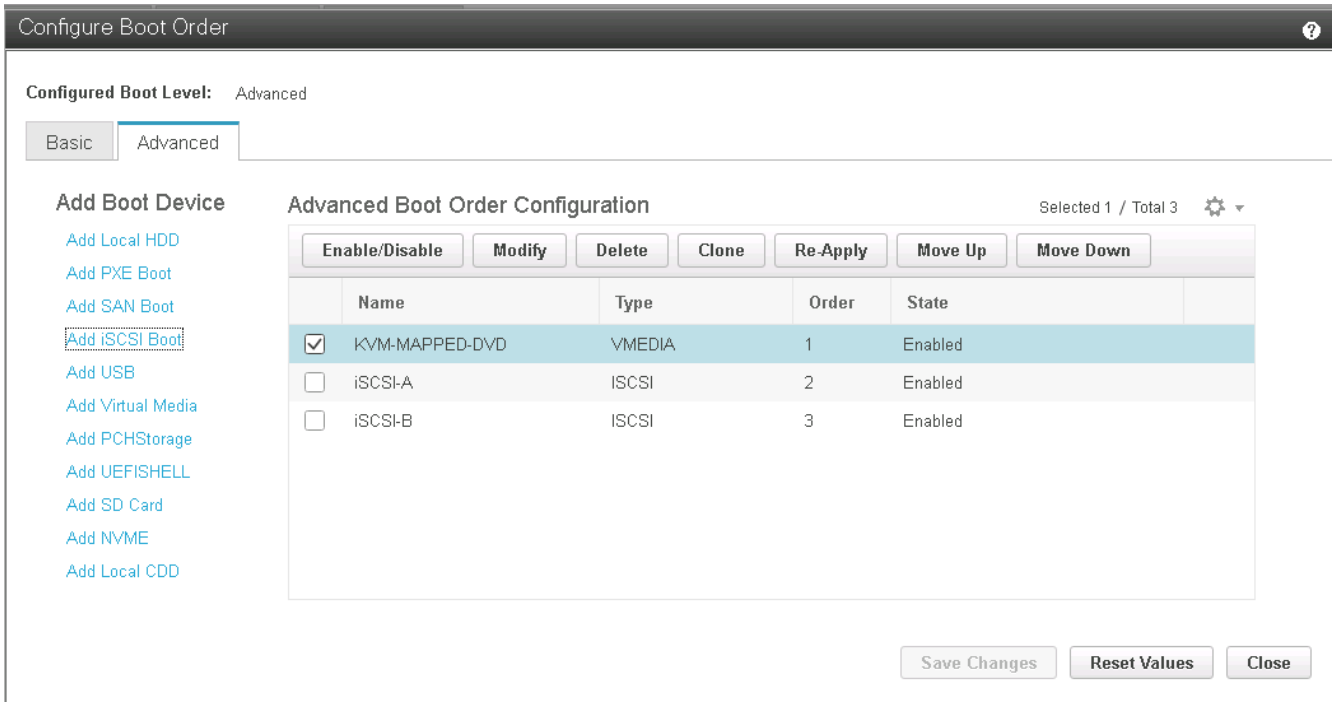
상태: 활성화됨

순서: 3

슬롯: mLOM

포트: 3

4. 장치 추가를 클릭합니다.
5. 변경 내용 저장 을 클릭한 다음 닫기 를 클릭합니다.



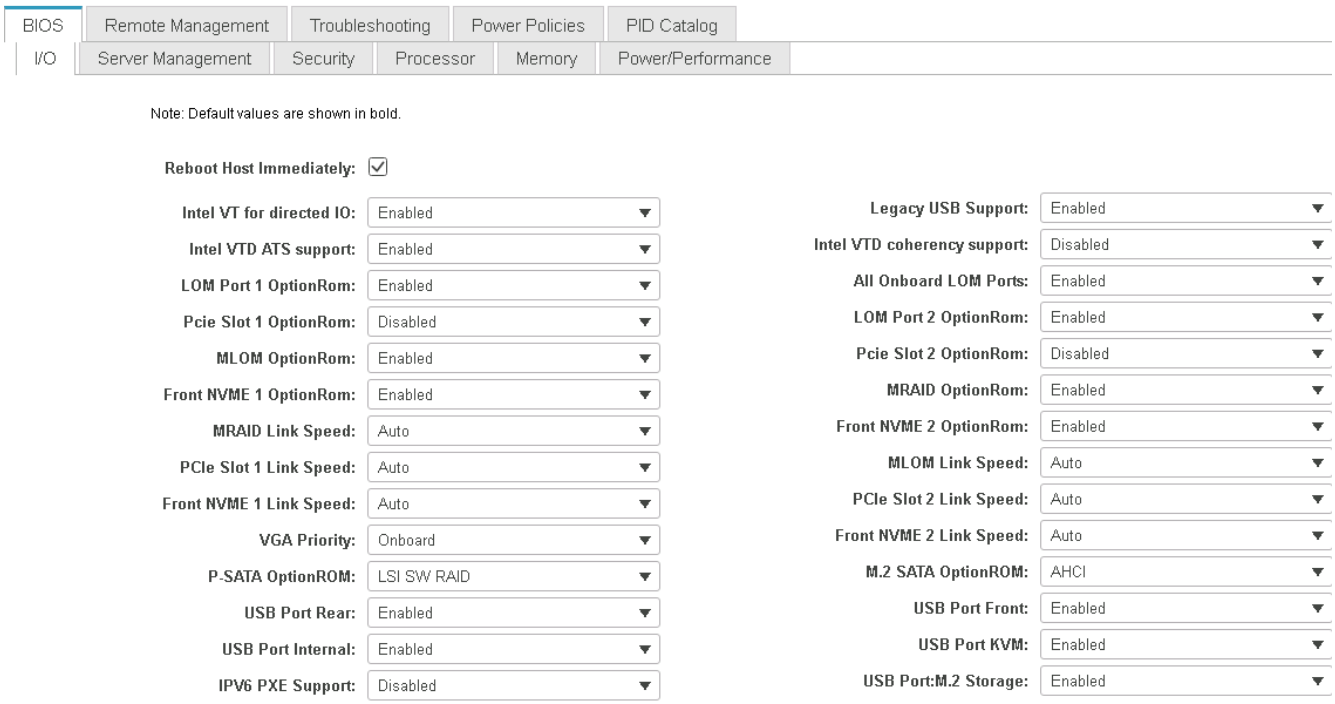
6. 새 부팅 순서로 부팅하려면 서버를 재부팅합니다.

RAID 컨트롤러 비활성화**(**있는 경우**)**

C 시리즈 서버에 RAID 컨트롤러가 포함되어 있는 경우 다음 단계를 수행하십시오. SAN 구성으로 부팅할 때 RAID 컨트롤러가 필요하지 않습니다. 선택적으로 서버에서 RAID 컨트롤러를 물리적으로 제거할 수도 있습니다.

1. Compute 탭의 CIMC의 왼쪽 탐색 창에서 BIOS를 클릭합니다.
2. Configure BIOS 를 선택합니다.

3. PCIe 슬롯: HBA 옵션 ROM으로 아래로 스크롤합니다.
4. 이 값이 아직 비활성화되지 않은 경우 비활성화로 설정합니다.

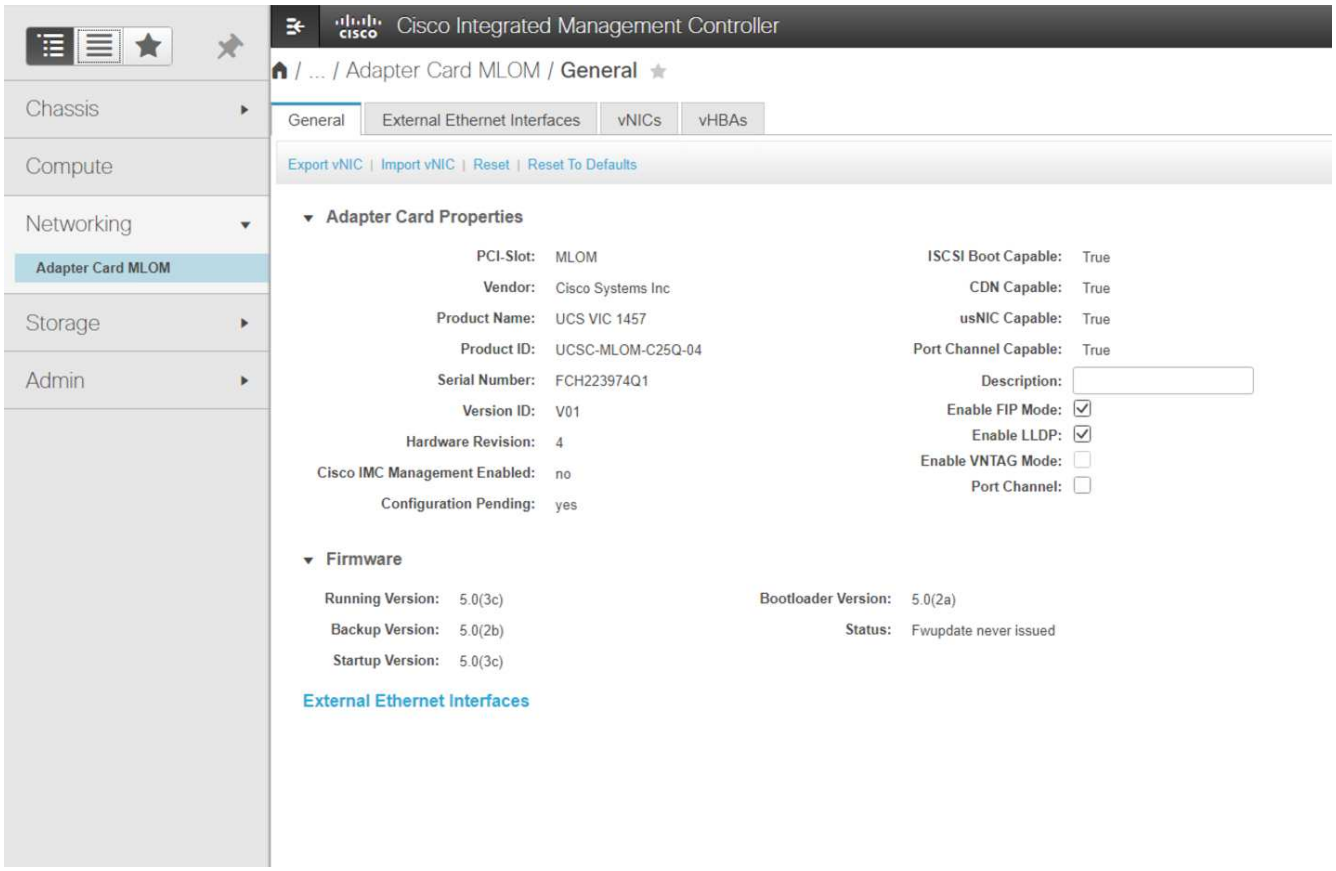


iSCSI 부트에 대해 **Cisco VIC1457**을 구성합니다

다음 구성 단계는 iSCSI 부트에 대한 Cisco VIC 1457에 대한 것입니다.

> 포트 0, 1, 2 및 3 간의 기본 포트 채널링을 해제해야 4개의 개별 포트를 구성할 수 있습니다. 포트 채널링이 꺼져 있지 않으면 VIC 1457에 대해 포트 두 개만 나타납니다. CIMC에서 포트 채널을 설정하려면 다음 단계를 완료하십시오.

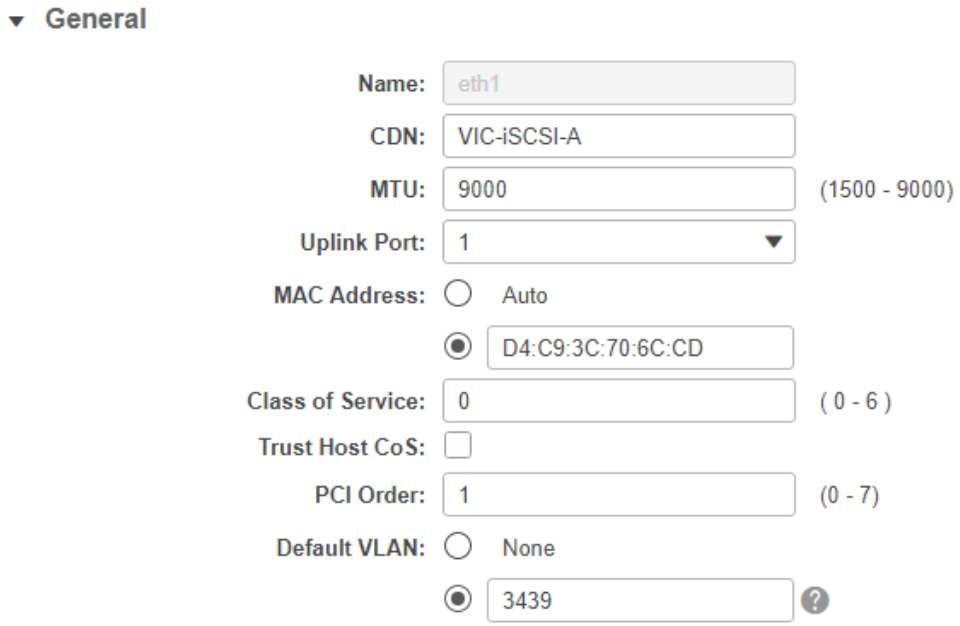
1. 네트워킹 탭에서 어댑터 카드 mLOM을 클릭합니다.
2. 일반 탭에서 포트 채널을 선택 취소합니다.
3. 변경 내용을 저장하고 CIMC를 재부팅합니다.



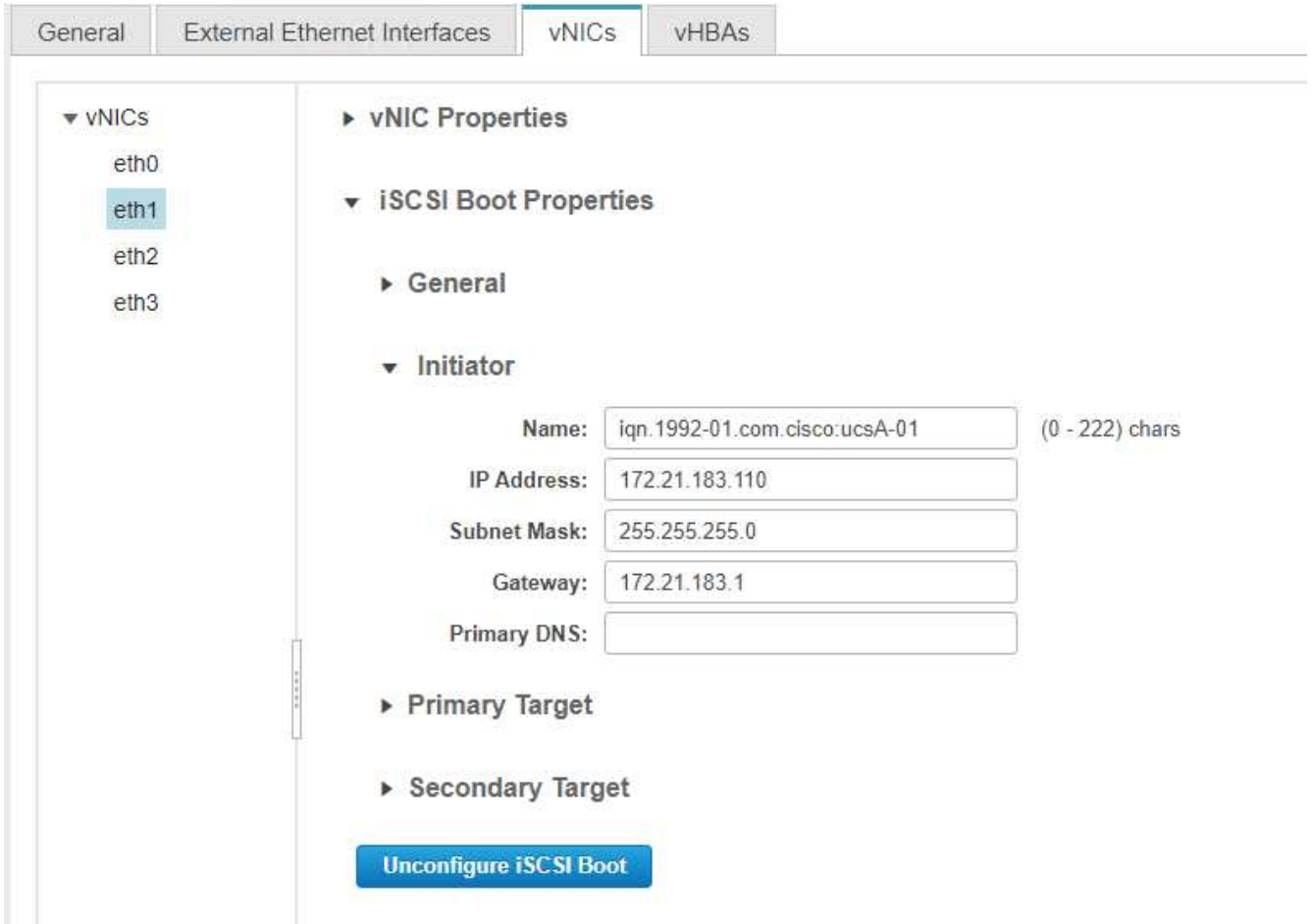
iSCSI vNIC를 생성합니다

iSCSI vNIC를 생성하려면 다음 단계를 수행하십시오.

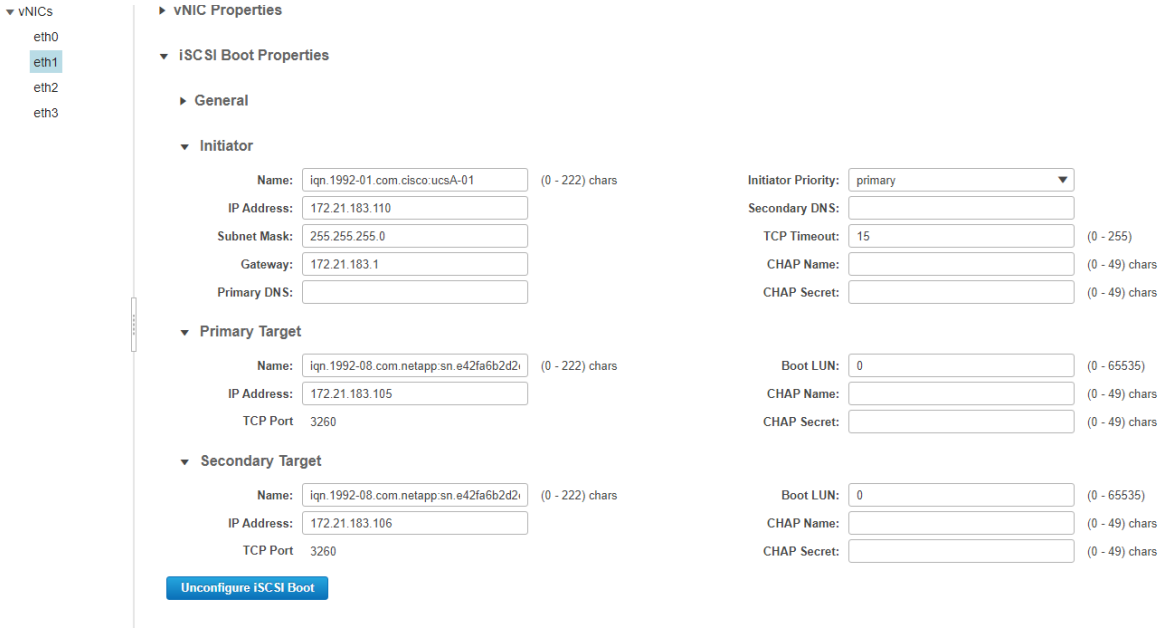
1. 네트워킹 탭에서 어댑터 카드 mLOM 을 클릭합니다.
2. vNIC 추가를 클릭하여 vNIC를 생성합니다.
3. vNIC 추가 섹션에서 다음 설정을 입력합니다.
   - 이름: eth1
   - CDN 이름: iSCSI-vNIC-A
   - MTU: 9000
   - 기본 VLAN:<<var_iscsi_vlan_a>>'입니다
   - VLAN 모드: 트렁크
   - PXE 부팅 활성화: 확인
4. vNIC 추가 를 클릭한 다음 확인 을 클릭합니다.
5. 이 과정을 반복하여 두 번째 vNIC를 추가합니다.
   - vNIC eth3의 이름을 지정합니다.
   - CDN 이름: iSCSI-vNIC-B
   - VLAN으로 '<<var_iscsi_vlan_b>>'를 입력합니다.
   - 업링크 포트를 3으로 설정합니다.



6. 왼쪽에서 vNIC eth1을 선택합니다.



7. iSCSI 부트 속성에서 이니시에이터 세부 정보를 입력합니다.
   - 이름:<<var_ucsa_initiator_name_a>>'
   - IP 주소: "<<var_esxi_hostA_iscsiA_ip>>"
   - 서브넷 마스크: "<<var_esxi_hostA_iscsiA_mask>>"
   - 게이트웨이: "\<<var_esxi_hostA_iscsiA_gateway>>"



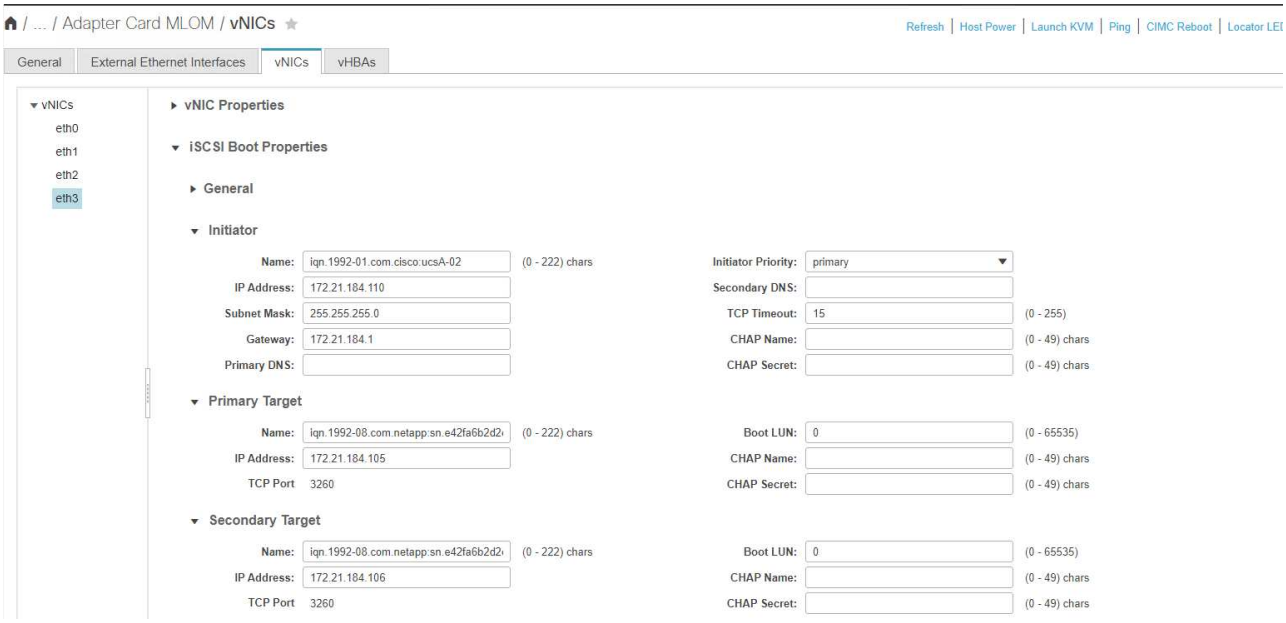
8. 기본 타겟 세부 정보를 입력합니다.
   - 이름: 인프라 SVM의 IQN 번호입니다
   - IP 주소: iSCSI_liff 01a의 IP 주소입니다
   - 부팅 LUN: 0
9. 2차 타겟 세부 정보를 입력합니다.
   - 이름: 인프라 SVM의 IQN 번호입니다
   - IP 주소: iscsi_lif02a 의 IP 주소입니다
   - 부팅 LUN: 0

> "vserver iscsi show" 명령을 실행하여 스토리지 IQN 번호를 확인할 수 있습니다.

> 각 vNIC의 IQN 이름을 기록해야 합니다. 나중에 필요한 단계일 수 있습니다. 또한 이니시에이터의 IQN 이름은 각 서버 및 iSCSI vNIC에 대해 고유해야 합니다.

10. 변경 내용 저장 을 클릭합니다.
11. vNIC eth3을 선택하고 호스트 이더넷 인터페이스 섹션 상단에 있는 iSCSI 부트 버튼을 클릭합니다.
12. 이 과정을 반복하여 eth3을 구성합니다.
13. 이니시에이터 세부 정보를 입력합니다.

- 이름:<<var_ucsa_initiator_name_b>>'
- IP 주소: "<<var_esxi_hostB_iscsib_ip>>"
- 서브넷 마스크: "<<var_esxi_hostB_iscsib_mask>>"
- 게이트웨이:\<<var_esxi_hostB_iscsib_gateway>'



14. 기본 타겟 세부 정보를 입력합니다.
    - 이름: 인프라 SVM의 IQN 번호입니다
    - IP 주소: iSCSI_liff 01b의 IP 주소입니다
    - 부팅 LUN: 0
15. 2차 타겟 세부 정보를 입력합니다.
    - 이름: 인프라 SVM의 IQN 번호입니다
    - IP 주소: iSCSI_liff 02b의 IP 주소입니다
    - 부팅 LUN: 0

> "vserver iscsi show" 명령을 사용하여 스토리지 IQN 번호를 가져올 수 있습니다.

> 각 vNIC의 IQN 이름을 기록해야 합니다. 나중에 필요한 단계일 수 있습니다.

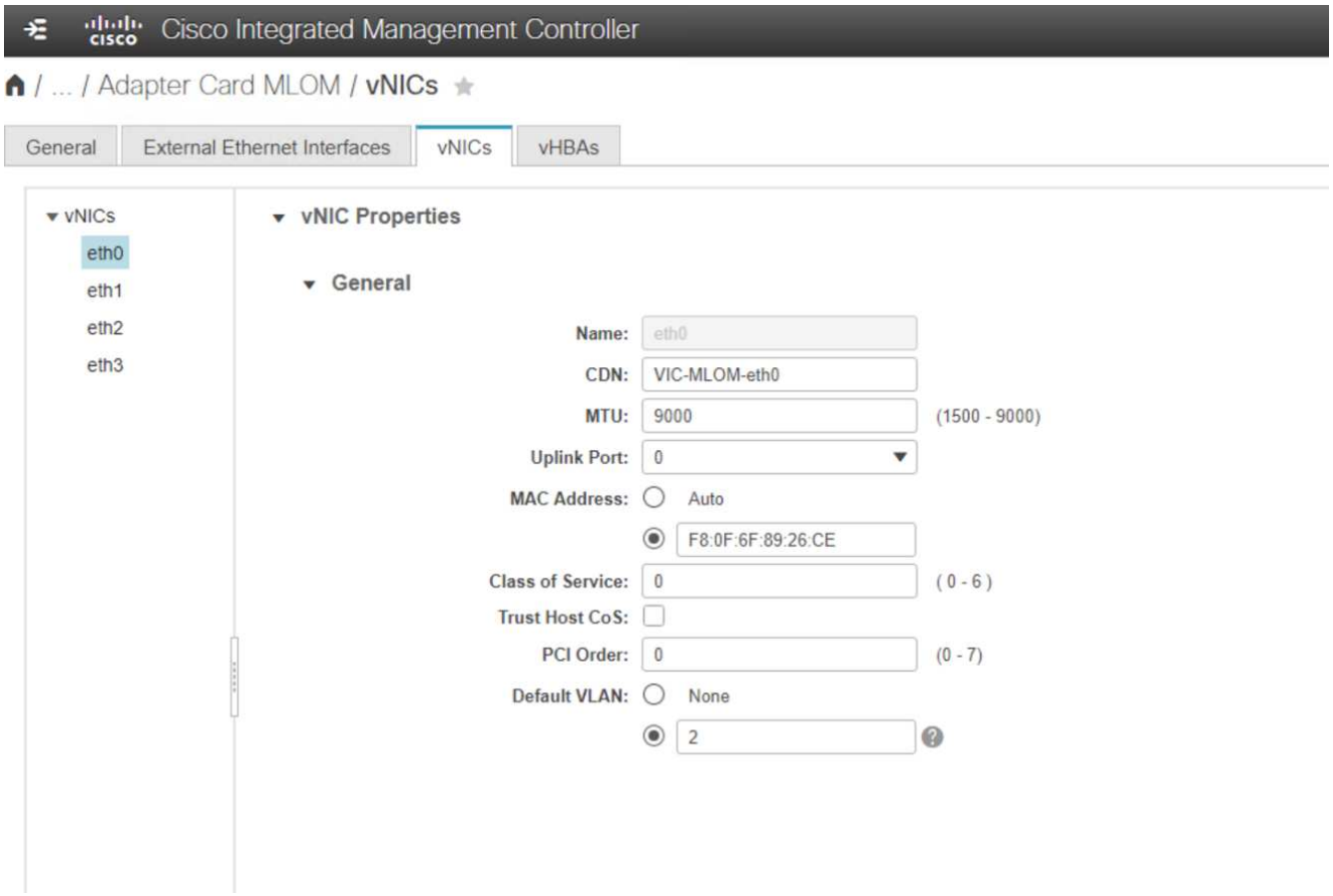
16. 변경 내용 저장 을 클릭합니다.
17. 이 프로세스를 반복하여 Cisco UCS 서버 B에 대한 iSCSI 부팅을 구성합니다

ESXi용 **vNIC**를 구성합니다

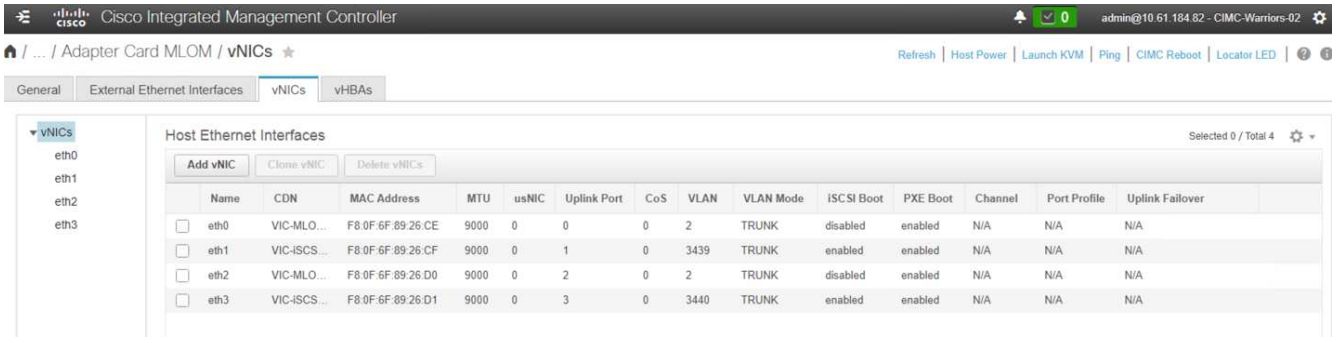
ESXi용 vNIC를 구성하려면 다음 단계를 수행하십시오.

1. CIMC 인터페이스 브라우저 창에서 인벤토리 를 클릭한 다음 오른쪽 창에서 Cisco VIC 어댑터 를 클릭합니다.

2. 네트워킹 > 어댑터 카드 mLOM 에서 vNIC 탭을 선택한 다음 아래에서 vNIC를 선택합니다.
3. eth0 을 선택하고 속성 을 클릭합니다.
4. MTU를 9000으로 설정합니다. 변경 내용 저장 을 클릭합니다.
5. VLAN을 네이티브 VLAN 2로 설정합니다.



6. eth1에 대해 3단계와 4단계를 반복하여 업링크 포트가 eth1에 대해 1로 설정되어 있는지 확인합니다.



이 절차는 각 초기 Cisco UCS 서버 노드 및 환경에 추가된 각 추가 Cisco UCS 서버 노드에 대해 반복해야 합니다.

"다음은 NetApp AFF 스토리지 구축 절차(2부)입니다."

NetApp AFF 스토리지 구축 절차(2부)

ONTAP SAN 부팅 스토리지를 설정합니다

iSCSI igroup을 생성합니다

이 단계를 위해서는 서버 구성에서 iSCSI 이니시에이터 IQN이 필요합니다.

igroup을 생성하려면 클러스터 관리 노드의 SSH 연결에서 다음 명령을 실행합니다. 이 단계에서 만든 3개의 igroup을 보려면 'igroup show' 명령을 실행합니다.

```
igroup create –vserver Infra-SVM –igroup VM-Host-Infra-A –protocol iscsi
–ostype vmware –initiator <<var_vm_host_infra_a_iSCSI-
A_vNIC_IQN>>,<<var_vm_host_infra_a_iSCSI-B_vNIC_IQN>>
igroup create –vserver Infra-SVM –igroup VM-Host-Infra-B –protocol iscsi
–ostype vmware –initiator <<var_vm_host_infra_b_iSCSI-
A_vNIC_IQN>>,<<var_vm_host_infra_b_iSCSI-B_vNIC_IQN>>
```

Cisco UCS C-Series 서버를 추가할 때는 이 단계를 완료해야 합니다.

부팅 LUN을 igroup에 매핑합니다

```
To map boot LUNs to igroups, run the following commands from the cluster
management SSH connection:
lun map –vserver Infra-SVM –volume esxi_boot –lun VM-Host-Infra-A –igroup
VM-Host-Infra-A –lun-id 0
lun map –vserver Infra-SVM –volume esxi_boot –lun VM-Host-Infra-B –igroup
VM-Host-Infra-B –lun-id 0
```

Cisco UCS C-Series 서버를 추가할 때는 이 단계를 완료해야 합니다.

"다음: VMware vSphere 6.7U2 구축 절차"

VMware vSphere 6.7U2 구축 절차

이 섹션에서는 FlexPod Express 구성에 VMware ESXi 6.7U2를 설치하기 위한 절차를 자세히 설명합니다. 다음 구현 절차는 이전 섹션에서 설명한 환경 변수를 포함하도록 커스터마이징되었습니다.

이러한 환경에 VMware ESXi를 설치하는 방법은 여러 가지가 있습니다. 이 절차에서는 Cisco UCS C-Series 서버용 CIMC 인터페이스의 가상 KVM 콘솔과 가상 미디어 기능을 사용하여 원격 설치 미디어를 각 개별 서버에 매핑합니다.

이 절차는 Cisco UCS 서버 A 및 Cisco UCS 서버 B에 대해 완료되어야 합니다

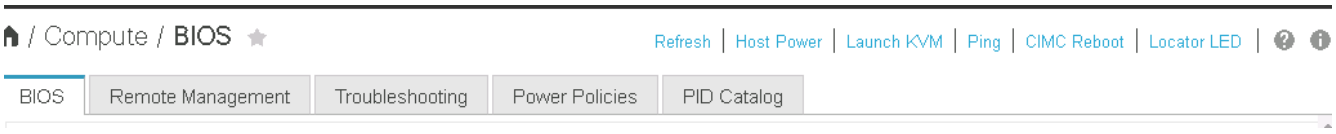
클러스터에 추가된 노드에 대해 이 절차를 완료해야 합니다.

Cisco UCS C-Series 독립 실행형 서버에 대한 CIMC 인터페이스에 로그인합니다

다음 단계에서는 Cisco UCS C-Series 독립 실행형 서버의 CIMC 인터페이스에 로그인하는 방법을 자세히 설명합니다. CIMC 인터페이스에 로그인하여 가상 KVM을 실행해야 관리자가 원격 미디어를 통해 운영 체제 설치를 시작할 수 있습니다.

모든 호스트

1. 웹 브라우저로 이동하고 Cisco UCS C-Series의 CIMC 인터페이스에 대한 IP 주소를 입력합니다. 이 단계에서는 CIMC GUI 애플리케이션이 시작됩니다.
2. 관리자의 사용자 이름과 자격 증명을 사용하여 CIMC UI에 로그인합니다.
3. 주 메뉴에서 서버 탭을 선택합니다.
4. Launch KVM Console을 클릭합니다.



5. 가상 KVM 콘솔에서 Virtual Media 탭을 선택합니다.
6. CD/DVD 매핑 을 선택합니다.

먼저 가상 디바이스 활성화 를 클릭해야 할 수도 있습니다. 메시지가 표시되면 이 세션 수락 을 선택합니다.

7. VMware ESXi 6.7U2 설치 관리자 ISO 이미지 파일을 찾아 이동하고 Open을 클릭합니다. 장치 매핑 을 클릭합니다.
8. Power 메뉴를 선택하고 Power Cycle System (Cold Boot) 을 선택합니다. 예 를 클릭합니다.

VMware ESXi를 설치합니다

다음 단계에서는 각 호스트에 VMware ESXi를 설치하는 방법을 설명합니다.

ESXi 6.7U2 Cisco 사용자 지정 이미지를 다운로드합니다

1. 로 이동합니다 "VMware vSphere 다운로드 페이지" 사용자 정의 ISO의 경우.
2. ESXi 6.7U2 설치 CD의 Cisco 사용자 지정 이미지 옆에 있는 다운로드로 이동 을 클릭합니다.
3. ESXi 6.7U2 설치 CD(ISO)용 Cisco 사용자 지정 이미지를 다운로드합니다.
4. 시스템이 부팅되면 VMware ESXi 설치 미디어의 존재 여부가 자동으로 감지됩니다.
5. 나타나는 메뉴에서 VMware ESXi 설치 프로그램을 선택합니다. 설치 프로그램이 로드되는데, 이 작업은 몇 분 정도 걸릴 수 있습니다.
6. 설치 프로그램 로드가 완료된 후 Enter 키를 눌러 설치를 계속합니다.
7. 최종 사용자 사용권 계약을 읽은 후 동의하고 F11 키를 눌러 설치를 계속합니다.

8. 이전에 ESXi용 설치 디스크로 설정된 NetApp LUN을 선택하고 Enter 키를 눌러 설치를 계속합니다.

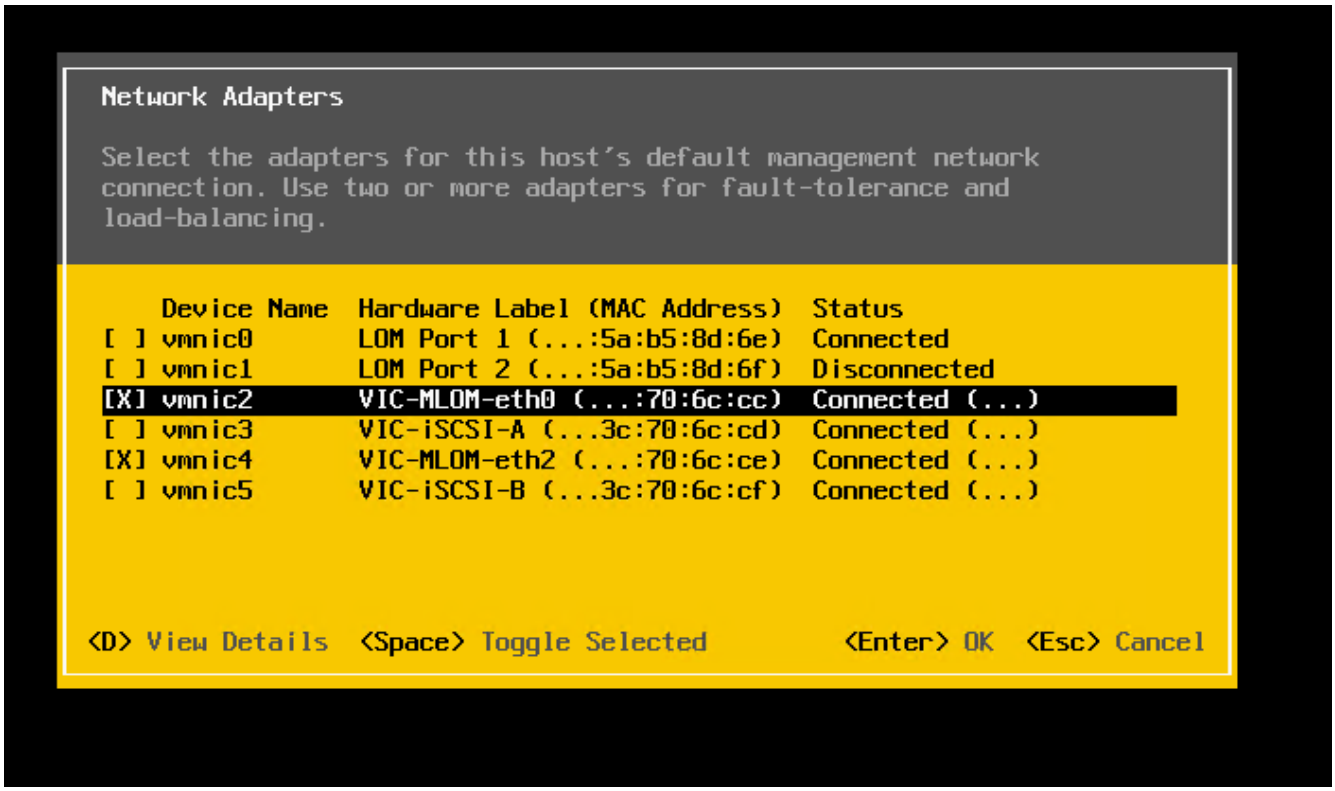
9. 적절한 자판 배열을 선택하고 Enter 키를 누릅니다.
10. 루트 암호를 입력 및 확인하고 Enter 키를 누릅니다.
11. 볼륨에서 기존 파티션이 제거된다는 경고 메시지가 표시됩니다. F11 키를 눌러 설치를 계속합니다. ESXi 설치 후 서버가 재부팅됩니다.

VMware ESXi 호스트 관리 네트워킹을 설정합니다

다음 단계에서는 각 VMware ESXi 호스트의 관리 네트워크를 추가하는 방법을 설명합니다.

모든 호스트

1. 서버 재부팅이 완료된 후 F2 키를 눌러 시스템 커스터마이징 옵션을 시작합니다.
2. root라는 로그인 이름과 이전에 설치 과정에서 입력한 루트 암호를 사용하여 로그인합니다.
3. Configure Management Network 옵션을 선택합니다.
4. Network Adapters 를 선택하고 Enter 키를 누릅니다.
5. vSwitch0에 대해 원하는 포트를 선택합니다. Enter 키를 누릅니다.
6. CIMC의 eth0 및 eth1에 해당하는 포트를 선택합니다.



7. VLAN (optional)을 선택하고 Enter 키를 누릅니다.
8. VLAN ID '<<mgmt_vlan_id>>'를 입력합니다. Enter 키를 누릅니다.
9. Configure Management Network 메뉴에서 IPv4 Configuration을 선택하여 관리 인터페이스의 IP 주소를 구성합니다. Enter 키를 누릅니다.
10. 화살표 키를 사용하여 정적 IPv4 주소 설정 을 강조 표시하고 스페이스바를 사용하여 이 옵션을 선택합니다.
11. VMware ESXi 호스트 "\< ESXi_host_mgmt_ip>>"를 관리하기 위한 IP 주소를 입력합니다.
12. VMware ESXi 호스트 "\< ESXi_host_mgmt_netmask>"의 서브넷 마스크를 입력합니다.
13. VMware ESXi 호스트 '\< ESXi_host_mgmt_gateway>'의 기본 게이트웨이를 입력합니다.
14. Enter 키를 눌러 IP 구성의 변경 사항을 적용합니다.
15. IPv6 구성 메뉴로 들어갑니다.
16. 스페이스바를 사용하여 IPv6 사용(재시작 필요) 옵션을 선택 취소하여 IPv6을 사용하지 않도록 설정합니다. Enter 키를 누릅니다.
17. DNS 설정을 구성하는 메뉴로 들어갑니다.
18. IP 주소는 수동으로 할당되므로 DNS 정보도 수동으로 입력해야 합니다.
19. Primary DNS 서버의 IP 주소 "\< nameserver_ip>>"를 입력합니다.
20. (선택 사항) 보조 DNS 서버의 IP 주소를 입력합니다.
21. VMware ESXi 호스트 이름 "\< ESXi_host_FQDN>"의 FQDN을 입력합니다.
22. Enter 키를 눌러 DNS 구성의 변경 사항을 적용합니다.
23. Esc 키를 눌러 Configure Management Network 하위 메뉴를 종료합니다.
24. Y 를 눌러 변경 사항을 확인하고 서버를 재부팅합니다.

25. 문제 해결 옵션 을 선택한 다음 ESXi Shell 및 SSH 활성화 를 선택합니다.

> 이러한 문제 해결 옵션은 고객의 보안 정책에 따라 정품 확인 후 비활성화할 수 있습니다.

26. Esc 키를 두 번 눌러 기본 콘솔 화면으로 돌아갑니다.
27. CIMC Macros > Static Macros > Alt-F 드롭다운 메뉴에서 Alt-F1 을 클릭합니다.
28. ESXi 호스트에 대한 올바른 자격 증명을 사용하여 로그인합니다.
29. 프롬프트에서 다음 esxcli 명령 목록을 순차적으로 입력하여 네트워크 연결을 활성화합니다.

```
esxcli network vswitch standard policy failover set -v vSwitch0 -a
vmnic2,vmnic4 -l iphash
```

ESXi 호스트를 구성합니다

다음 표의 정보를 사용하여 각 ESXi 호스트를 구성합니다.

세부 정보	상세 값
ESXi 호스트 이름입니다	ESXi_host_FQDN>>
ESXi 호스트 관리 IP입니다	ESXi_host_mgmt_ip>>
ESXi 호스트 관리 마스크입니다	ESXi_host_mgmt_netmask>>
ESXi 호스트 관리 게이트웨이	ESXi_host_mgmt_gateway>>
ESXi 호스트 NFS IP입니다	ESXi_host_nfs_ip>>
ESXi 호스트 NFS 마스크입니다	ESXi_host_nfs_netmask>>
ESXi 호스트 NFS 게이트웨이	ESXi_host_nfs_gateway>>
ESXi 호스트 vMotion IP입니다	ESXi_HOST_vMotion_IP>>
ESXi 호스트 vMotion 마스크	ESXi_host_vMotion_netmask>>
ESXi 호스트 vMotion 게이트웨이	ESXi_host_vMotion_gateway>>
ESXi 호스트 iSCSI - A IP	ESXi_host_iscsi-a_ip>>
ESXi 호스트 iSCSI - 마스크	ESXi_host_iscsi-a_netmask>>
ESXi 호스트 iSCSI - 게이트웨이	ESXi_host_iscsi-a_gateway>>
ESXi 호스트 iSCSI-B IP	ESXi_host_iscsi-B_ip>>
ESXi 호스트 iSCSI-B 마스크	ESXi_host_iscsi-B_netmask>>
ESXi 호스트 iSCSI-B 게이트웨이	ESXi_host_scsi-B_gateway>>

ESXi 호스트에 로그인합니다

ESXi 호스트에 로그인하려면 다음 단계를 수행하십시오.

1. 웹 브라우저에서 호스트의 관리 IP 주소를 엽니다.

2. 설치 프로세스 중에 지정한 암호 및 루트 계정을 사용하여 ESXi 호스트에 로그인합니다.
3. VMware 사용자 환경 개선 프로그램에 대한 설명을 읽어 보십시오. 적절한 응답을 선택한 후 OK(확인) 를 클릭합니다.

iSCSI 부트를 구성합니다

iSCSI 부트를 구성하려면 다음 단계를 수행하십시오.

1. 왼쪽에서 네트워킹 을 선택합니다.
2. 오른쪽에서 Virtual Switches 탭을 선택합니다.

3. iSciBootvSwitch 를 클릭합니다.
4. 설정 편집 을 선택합니다.
5. MTU를 9000으로 변경하고 저장 을 클릭합니다.
6. iSCSIBootPG 포트의 이름을 iSCSIBootPG-A로 바꿉니다

> 이 구성에서는 Vmnic3 및 vmnic5가 iSCSI 부팅에 사용됩니다. ESXi 호스트에 추가 NIC가 있는 경우 vmnic 번호가 다를 수 있습니다. iSCSI 부트에 사용되는 NIC를 확인하려면 CIMC의 iSCSI vNIC의 MAC 주소를 ESXi의 vmnics와 일치시킵니다.

7. 가운데 창에서 VMkernel NIC 탭을 선택합니다.
8. Add VMkernel NIC 를 선택합니다.
   a. iSciBootPG-B의 새 포트 그룹 이름을 지정합니다
   b. 가상 스위치에 대해 iSciBootvSwitch를 선택합니다.
   c. VLAN ID에 '<<iscsib_vlan_id>>'를 입력합니다.
   d. MTU를 9000으로 변경합니다.
   e. IPv4 설정 을 확장합니다.

f. 정적 설정을 선택합니다.

g. Address 에 "<<var_hosta_iscsib_ip>>"를 입력합니다.

h. 서브넷 마스크에 '<<var_hosta_iscsib_mask>>'를 입력합니다.

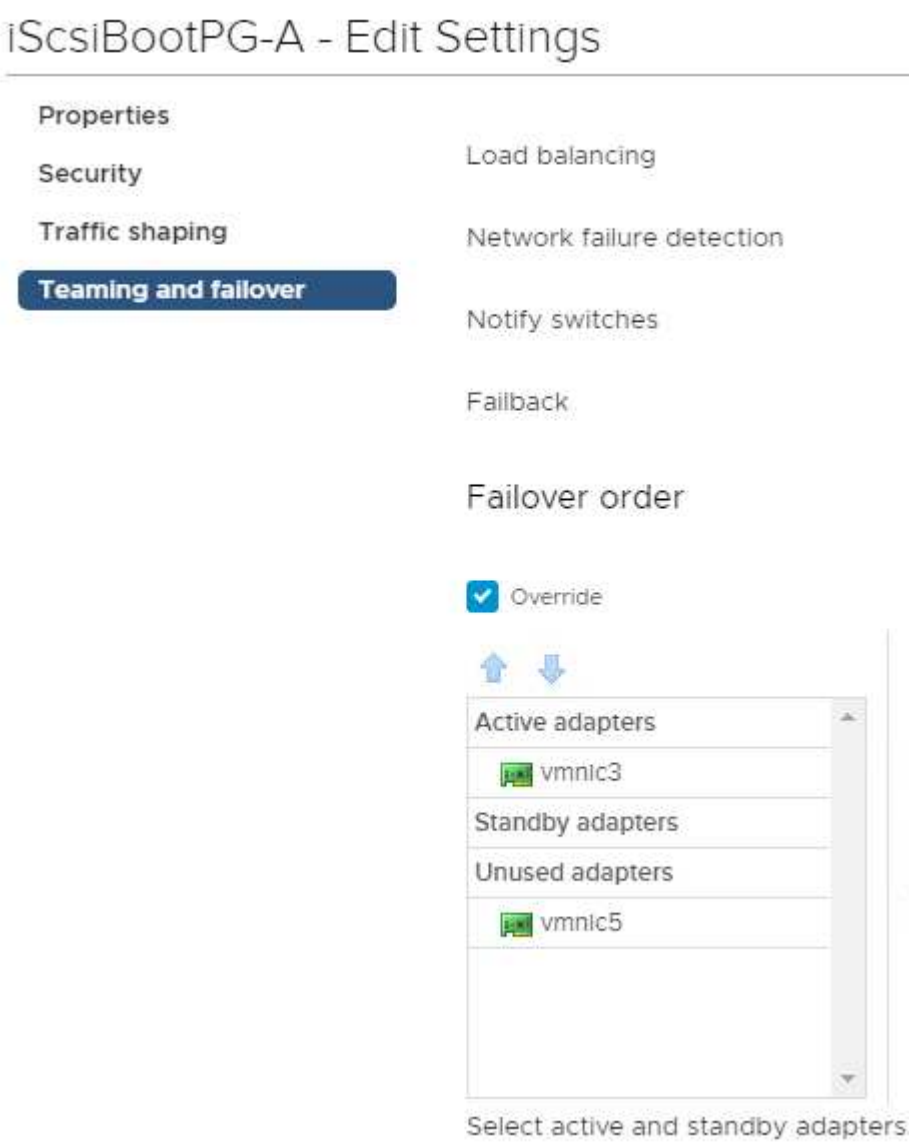
i. 생성 을 클릭합니다.

iSciBootPG-A에서 MTU를 9000으로 설정합니다

9. 페일오버를 설정하려면 다음 단계를 수행하십시오.

a. iSCSIBootPG-A > 계층화 및 페일오버 > 페일오버 순서 > Vmnic3에서 설정 편집 을 클릭합니다. Vmnic3이 활성 상태이고 vmnic5가 사용되지 않아야 합니다.

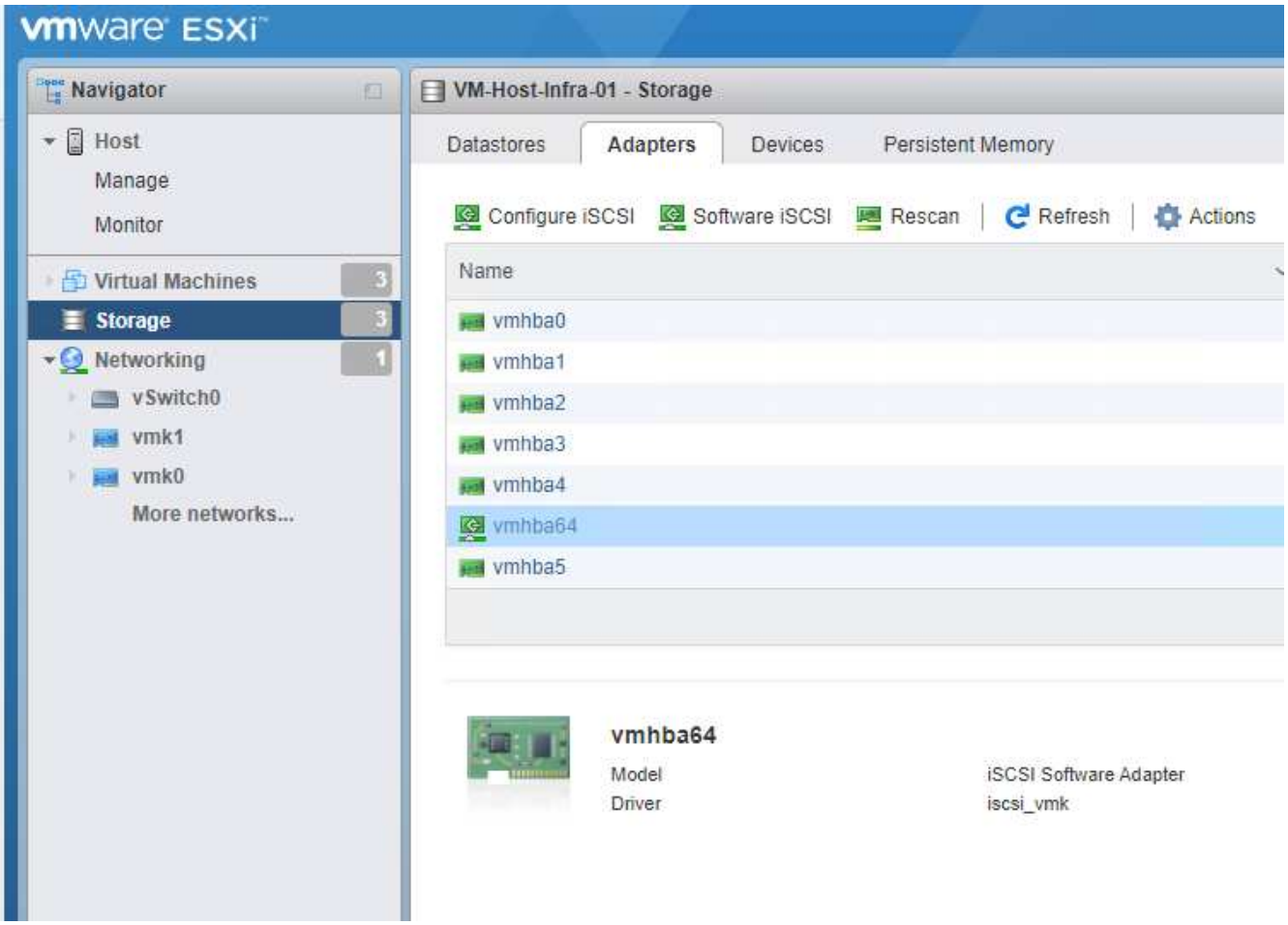
b. iSCSIBootPG-B > 팀 구성 및 장애 조치 > 장애 조치 순서 > Vmnic5에서 설정 편집 을 클릭합니다. Vmnic5는 활성 상태이고 vmnic3는 사용하지 않아야 합니다.



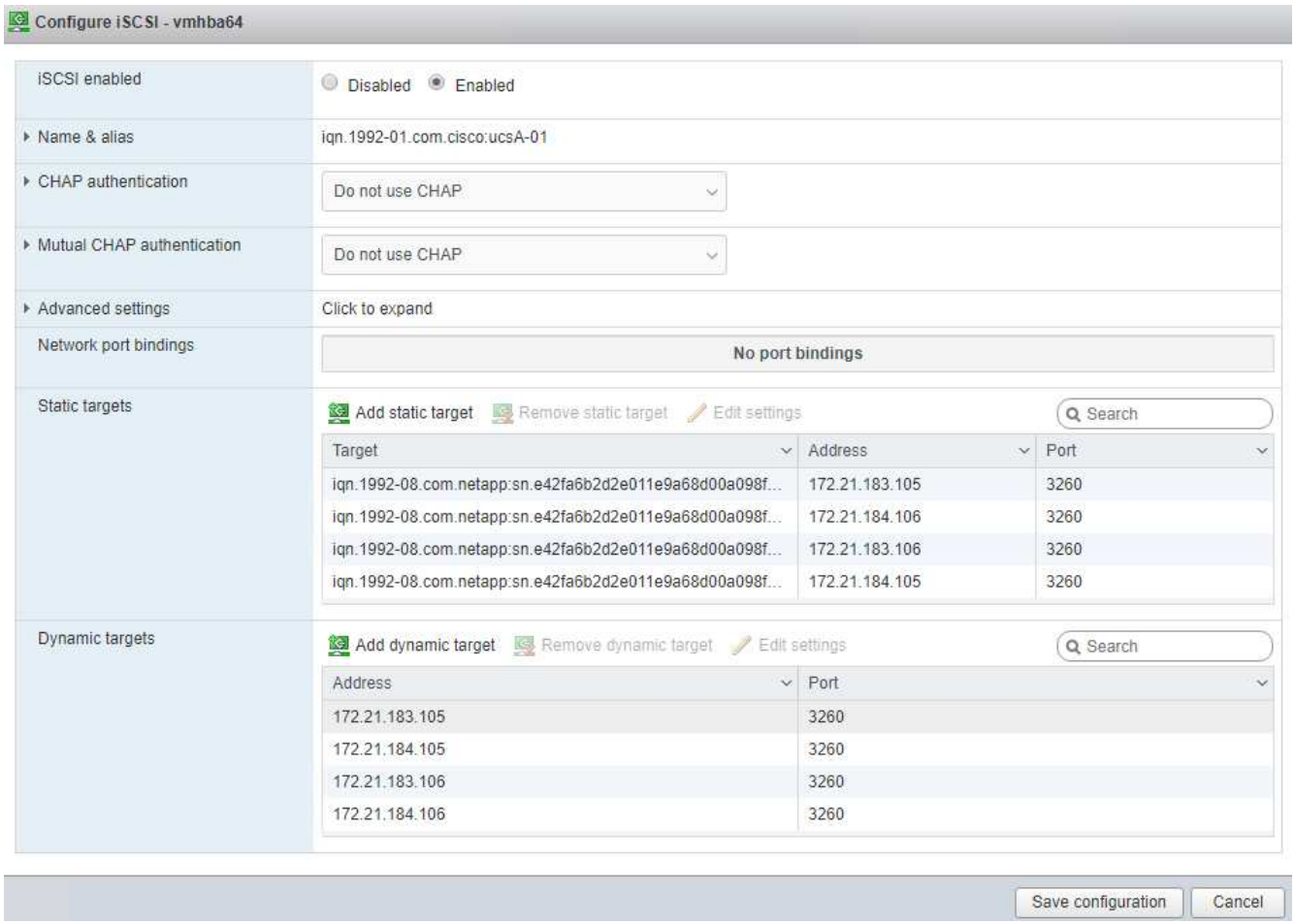
iSCSI 다중 경로를 구성합니다

ESXi 호스트에 iSCSI 다중 경로를 설정하려면 다음 단계를 수행하십시오.

1. 왼쪽 탐색 창에서 스토리지 를 선택합니다. 어댑터를 클릭합니다.
2. iSCSI 소프트웨어 어댑터를 선택하고 iSCSI 구성 을 클릭합니다.



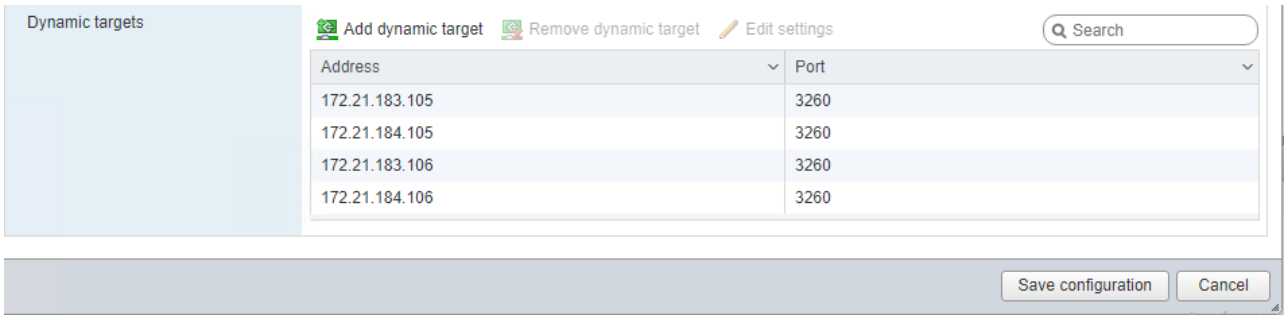
3. 동적 대상에서 동적 대상 추가를 클릭합니다.



4. IP 주소 'iscsi_lif01a'를 입력합니다.

   a. IP 주소 iscsi_liff 01b, iscsi_liff 02a, iscsi_liff 02b와 함께 이 과정을 반복합니다.

   b. 구성 저장 을 클릭합니다.



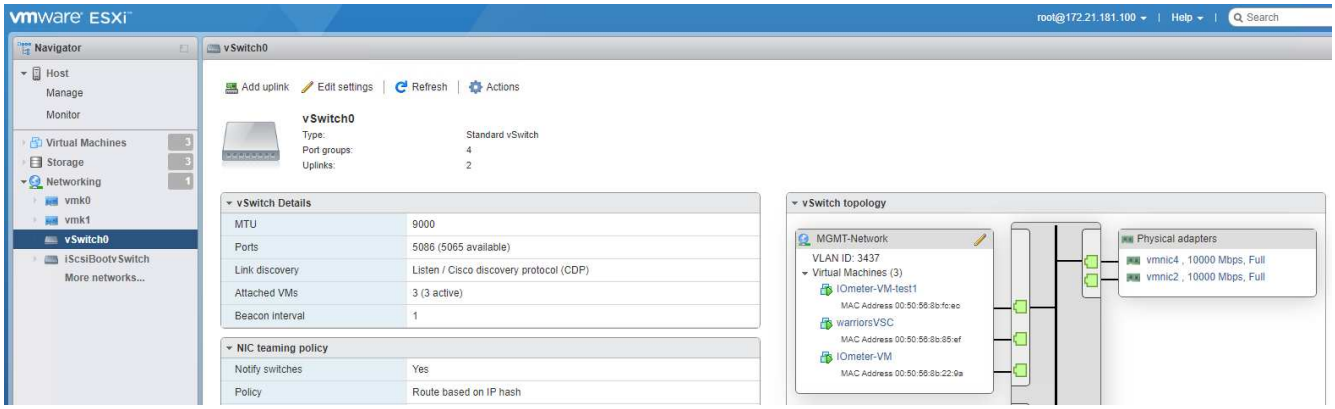
NetApp 클러스터에서 network interface show 명령을 실행하거나 System Manager의 네트워크 인터페이스 탭을 확인하여 iSCSI LIF IP 주소를 찾을 수 있습니다.

ESXi 호스트를 구성합니다

ESXi 부트를 구성하려면 다음 단계를 수행하십시오.

1. 왼쪽 탐색 창에서 네트워킹 을 선택합니다.

2. vSwitch0을 선택합니다.



3. 설정 편집 을 선택합니다.
4. MTU를 9000으로 변경합니다.
5. NIC 티밍을 확장하고 vmnic2 및 vmnic4가 활성으로 설정되어 있고 NIC 티밍과 장애 조치가 IP 해시를 기준으로 라우팅으로 설정되어 있는지 확인합니다.

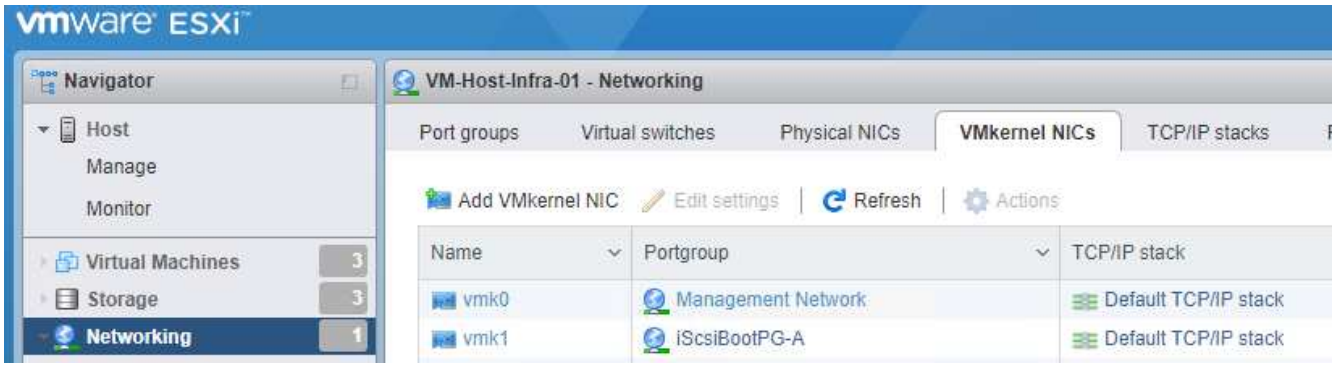
로드 밸런싱의 IP 해시 방법을 사용하려면 기본 물리적 스위치를 정적(모드 온) 포트 채널과 함께 SRC-DST-IP EtherChannel을 사용하여 올바르게 구성해야 합니다. 스위치 구성 오류로 인해 연결이 간헐적으로 끊길 수 있습니다. 이 경우 포트 채널 설정 문제를 해결하는 동안 Cisco 스위치에서 연결된 두 개의 업링크 포트 중 하나를 일시적으로 종료하여 ESXi 관리 vmkernel 포트로의 통신을 복구합니다.

포트 그룹과 **VMkernel NIC**를 구성합니다

포트 그룹과 VMkernel NIC를 구성하려면 다음 단계를 완료합니다.

1. 왼쪽 탐색 창에서 네트워킹 을 선택합니다.
2. 포트 그룹 탭을 마우스 오른쪽 단추로 클릭합니다.

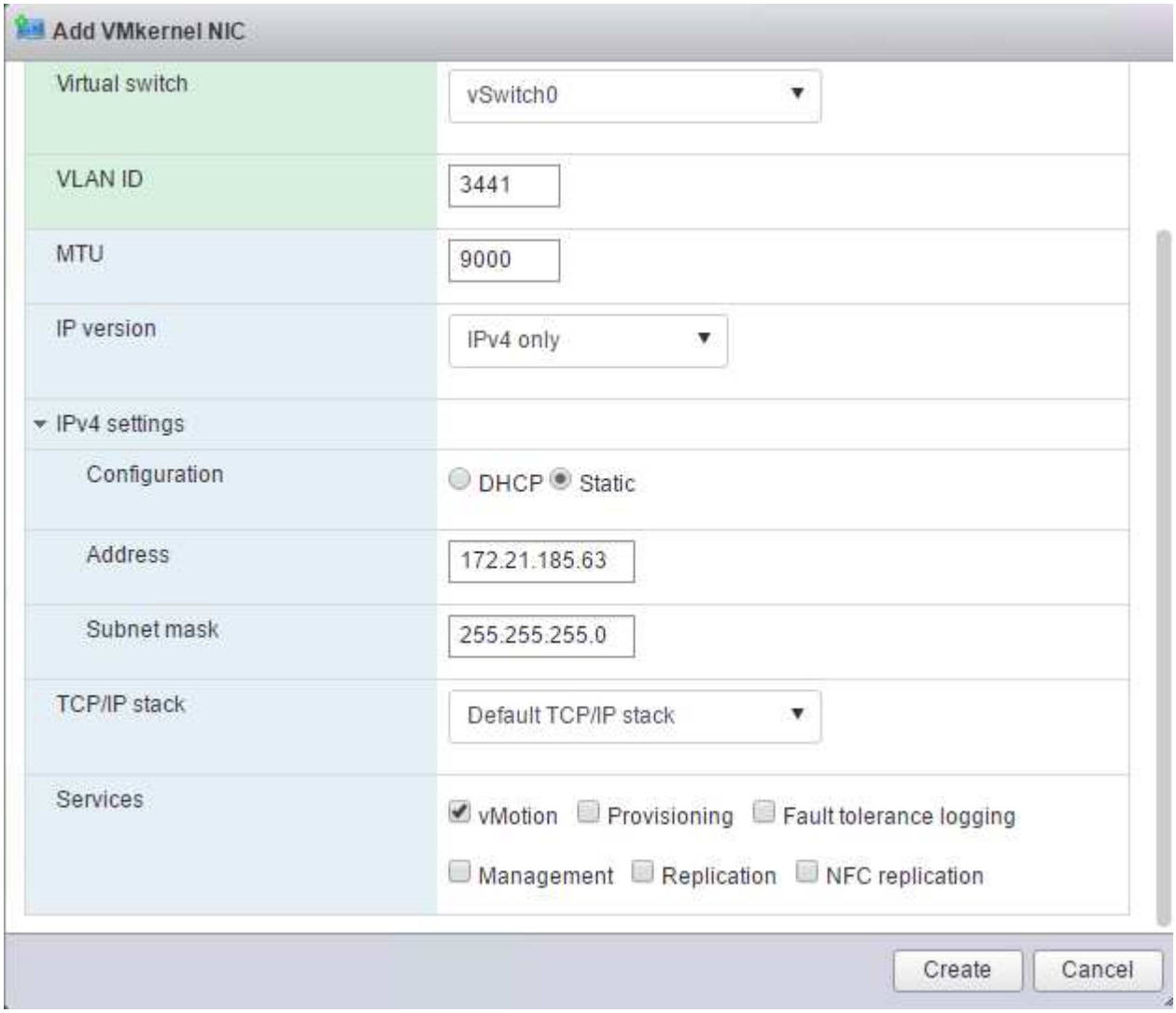
3. VM Network를 마우스 오른쪽 버튼으로 클릭하고 Edit를 선택합니다. VLAN ID를 '<<var_vm_traffic_vlan>>'로 변경합니다.
4. 포트 그룹 추가 를 클릭합니다.
    a. 포트 그룹의 이름을 MGMT-Network로 지정합니다.
    b. VLAN ID에 '<<mgmt_vlan>>'를 입력합니다.
    c. vSwitch0이 선택되어 있는지 확인합니다.
    d. 저장 을 클릭합니다.
5. VMkernel NIC 탭을 클릭합니다.



6. Add VMkernel NIC 를 선택합니다.
    a. 새 포트 그룹을 선택합니다.
    b. 포트 그룹의 이름을 NFS-Network로 지정합니다.
    c. VLAN ID에 '<<nfs_vlan_id>>'를 입력합니다.
    d. MTU를 9000으로 변경합니다.
    e. IPv4 설정 을 확장합니다.
    f. 정적 설정을 선택합니다.
    g. Address 에 "<<var_hosta_nfs_ip>>"를 입력합니다.
    h. 서브넷 마스크에 '<<var_hosta_nfs_mask>>'를 입력합니다.
    i. 생성 을 클릭합니다.
7. 이 프로세스를 반복하여 vMotion VMkernel 포트를 생성합니다.
8. Add VMkernel NIC 를 선택합니다.
    a. 새 포트 그룹을 선택합니다.
    b. 포트 그룹의 이름을 vMotion으로 지정합니다.
    c. VLAN ID에 '\< vMotion_vlan_id>>'를 입력합니다.
    d. MTU를 9000으로 변경합니다.
    e. IPv4 설정 을 확장합니다.
    f. 정적 설정을 선택합니다.
    g. Address 에 "<<var_hosta_vmotion_ip>>"를 입력합니다.

h. 서브넷 마스크에 '<<var_hosta_vmotion_mask>>'를 입력합니다.

i. IPv4 설정 후 vMotion 확인란이 선택되어 있는지 확인합니다.

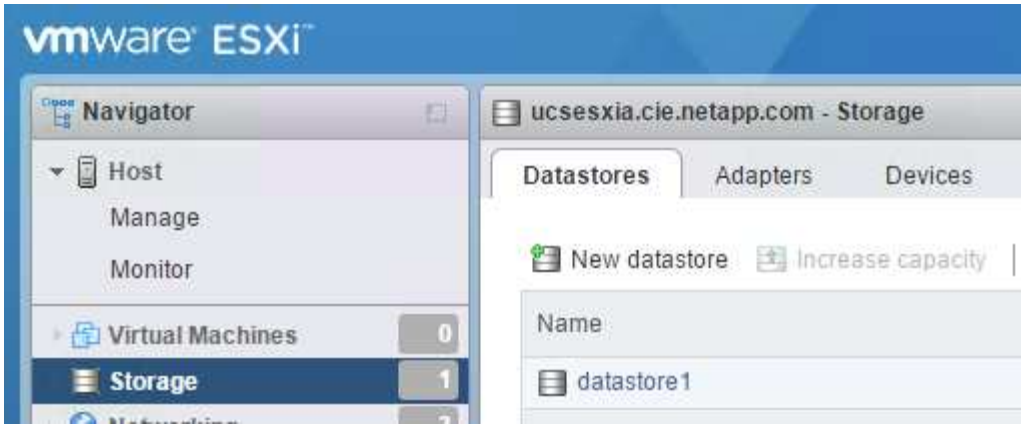


라이센싱에서 허용하는 경우 VMware vSphere 분산 스위치를 사용하는 등 여러 가지 방법으로 ESXi 네트워킹을 구성할 수 있습니다. 비즈니스 요구 사항을 충족하는 데 필요한 경우 FlexPod Express에서 대체 네트워크 구성이 지원됩니다.

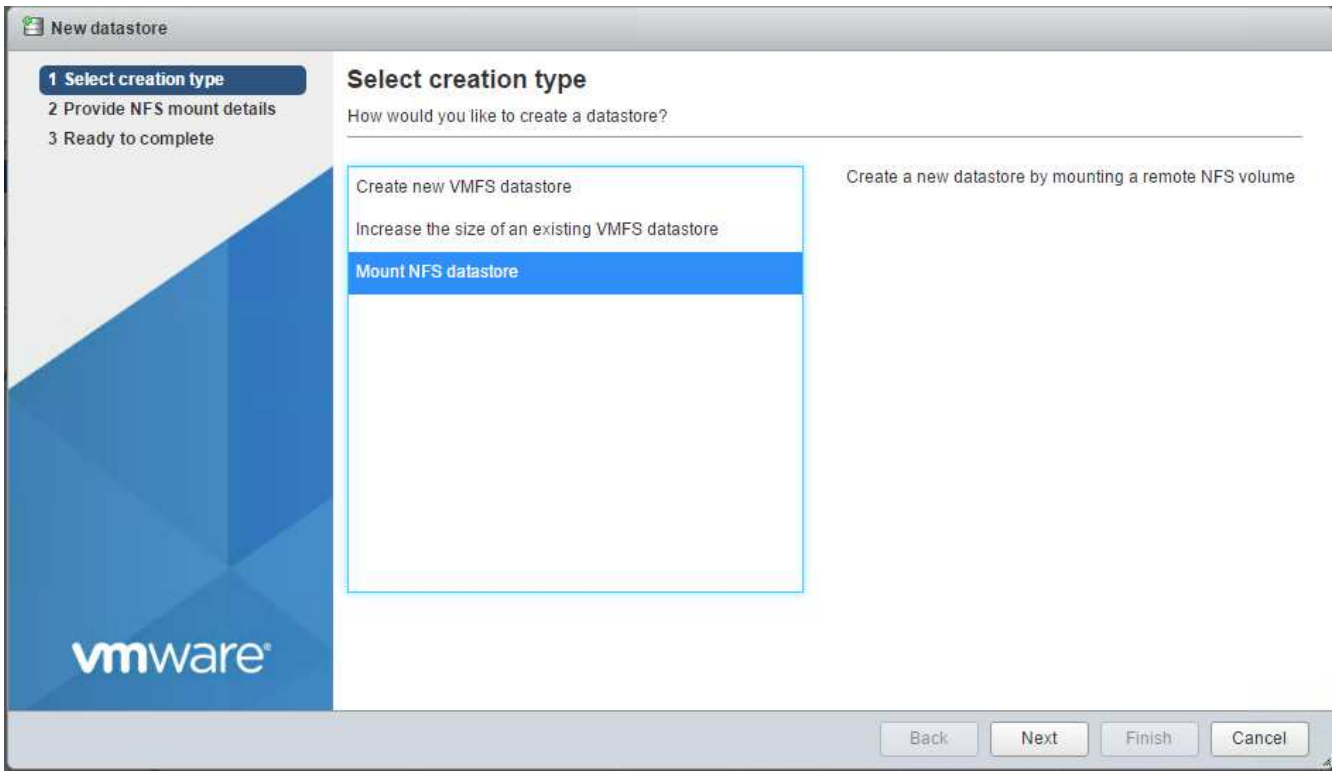
첫 번째 데이터 저장소를 마운트합니다

첫 번째로 마운트할 데이터스토어는 VM용 infra_datastore 데이터 저장소와 VM 스왑 파일을 위한 infra_swap 데이터 저장소입니다.

1. 왼쪽 탐색 창에서 스토리지 를 클릭한 다음 새 데이터 저장소 를 클릭합니다.



2. Mount NFS Datastore를 선택합니다.



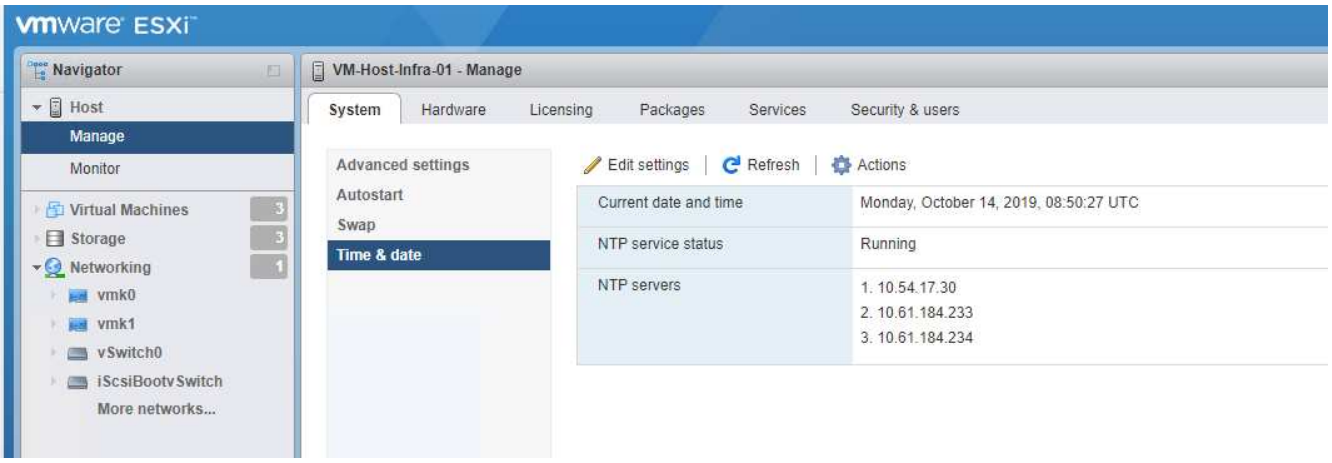
3. NFS 마운트 세부 정보 제공 페이지에 다음 정보를 입력합니다.
   - 이름: 'infra_datastore'
   - NFS 서버:\<<var_NodeA_nfs_lif>'
   - 공유: '/infra_datastore'
   - NFS 3이 선택되어 있는지 확인합니다.
4. 마침 을 클릭합니다. 최근 작업 창에서 작업이 완료된 것을 볼 수 있습니다.
5. 이 프로세스를 반복하여 'infra_swap' 데이터 저장소를 마운트합니다.
   - 이름: infra_swap
   - NFS 서버:\<<var_NodeA_nfs_lif>'
   - 공유: '/infra_swap'

◦ NFS 3이 선택되어 있는지 확인합니다.

NTP를 구성합니다

ESXi 호스트에 대해 NTP를 구성하려면 다음 단계를 수행하십시오.

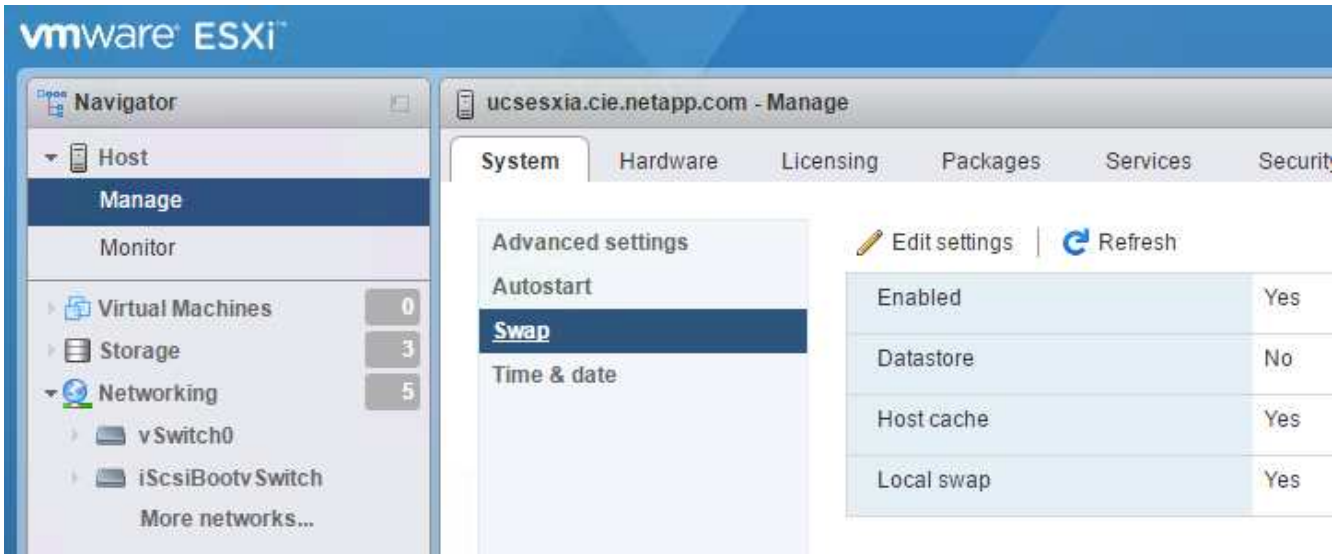
1. 왼쪽 탐색 창에서 관리 를 클릭합니다. 오른쪽 창에서 시스템 을 선택한 다음 시간 및 날짜 를 클릭합니다.
2. Use Network Time Protocol (Enable NTP Client) 을 선택합니다.
3. Start and Stop with Host 를 NTP 서비스 시작 정책으로 선택합니다.
4. NTP 서버로 '<<var_ntp>>'를 입력합니다. 여러 NTP 서버를 설정할 수 있습니다.
5. 저장 을 클릭합니다.



VM 스왑 파일 위치를 이동합니다

다음 단계에서는 VM 스왑 파일 위치를 이동하는 방법을 자세히 설명합니다.

1. 왼쪽 탐색 창에서 관리 를 클릭합니다. 오른쪽 창에서 시스템을 선택한 다음 바꾸기를 클릭합니다.



2. 설정 편집 을 클릭합니다. Datastore 옵션에서 infra_swap을 선택합니다.

3. 저장 을 클릭합니다.

"다음: VMware vCenter Server 6.7U2 설치 절차"

VMware vCenter Server 6.7U2 설치 절차

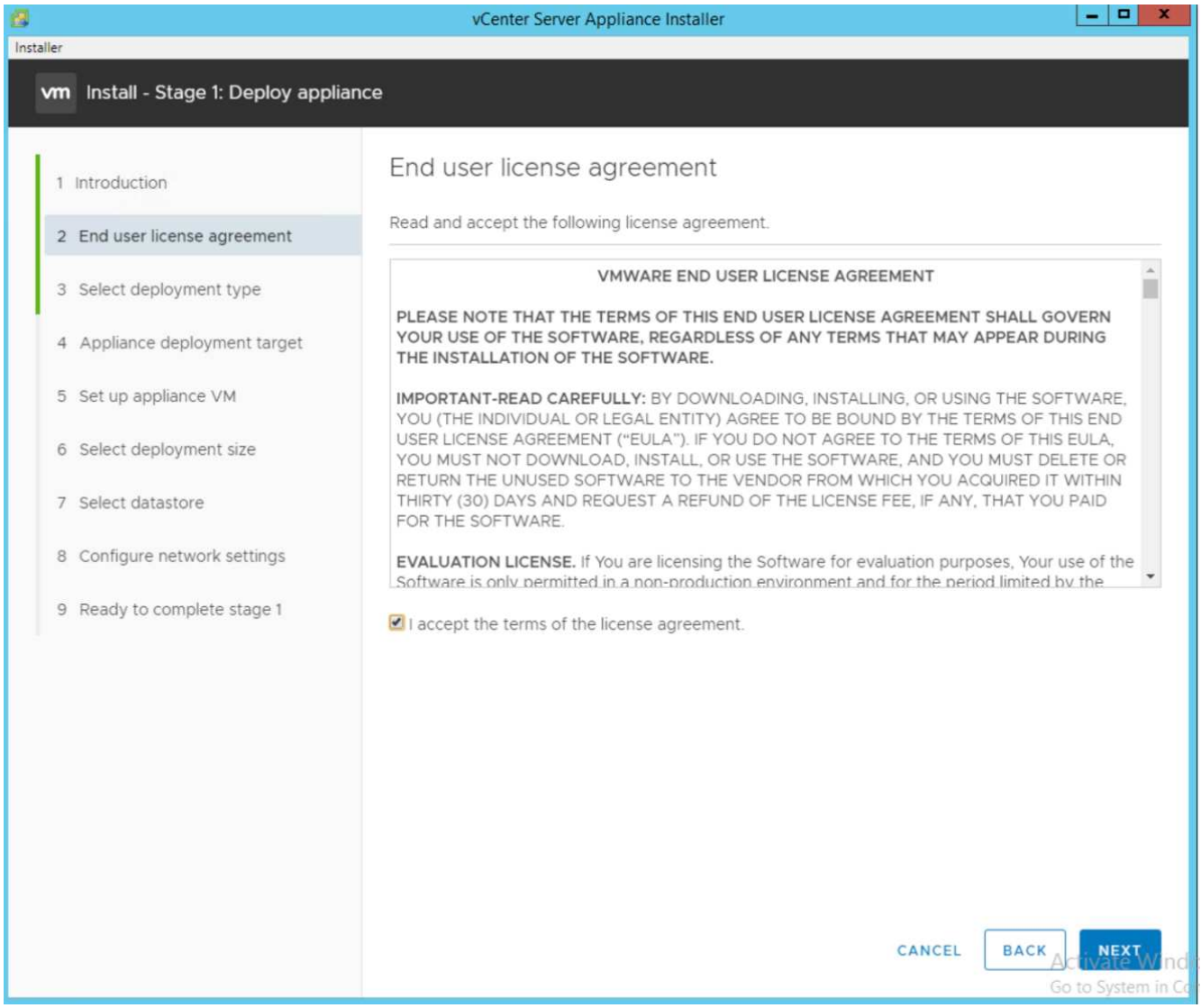
이 섹션에서는 FlexPod Express 구성에 VMware vCenter Server 6.7을 설치하는 절차를 자세히 설명합니다.

FlexPod Express는 VCSA(VMware vCenter Server Appliance)를 사용합니다.

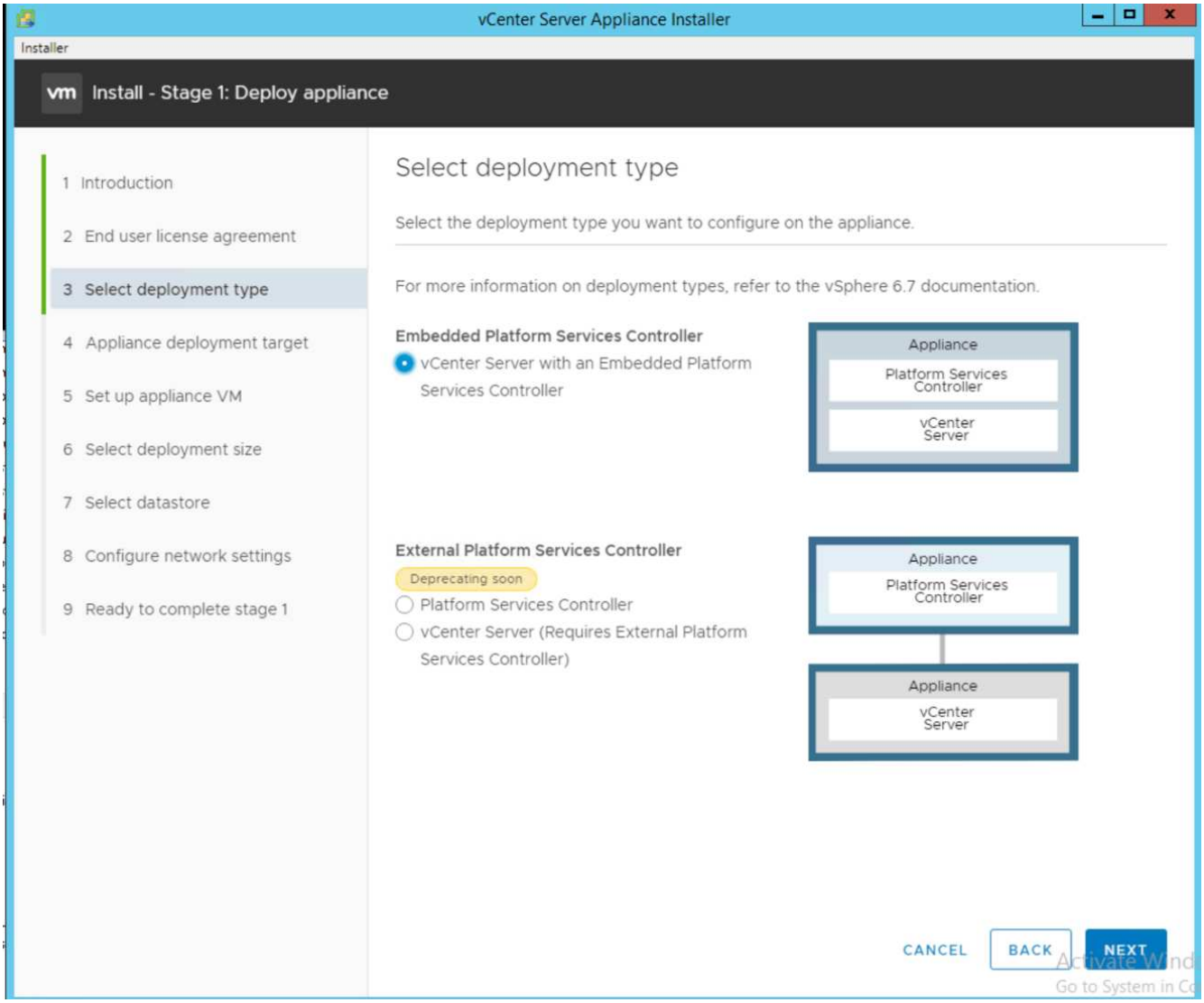
VMware vCenter Server Appliance를 다운로드합니다

VMware vCenter Server Appliance(VCSA)를 다운로드하려면 다음 단계를 수행하십시오.

1. VCSA를 다운로드합니다. ESXi 호스트를 관리할 때 vCenter Server 가져오기 아이콘을 클릭하여 다운로드 링크를 액세스합니다.
2. VMware 사이트에서 VCSA를 다운로드합니다.
3. Microsoft Windows vCenter Server 설치 가능한 가 지원되지만 VMware는 새로운 구축에 VCSA를 권장합니다.
4. ISO 이미지를 마운트합니다.
5. vcsa-UI-installer> Win32 디렉터리로 이동합니다. installer.exe를 두 번 클릭합니다.
6. 설치 를 클릭합니다.
7. 소개 페이지에서 다음 을 클릭합니다.

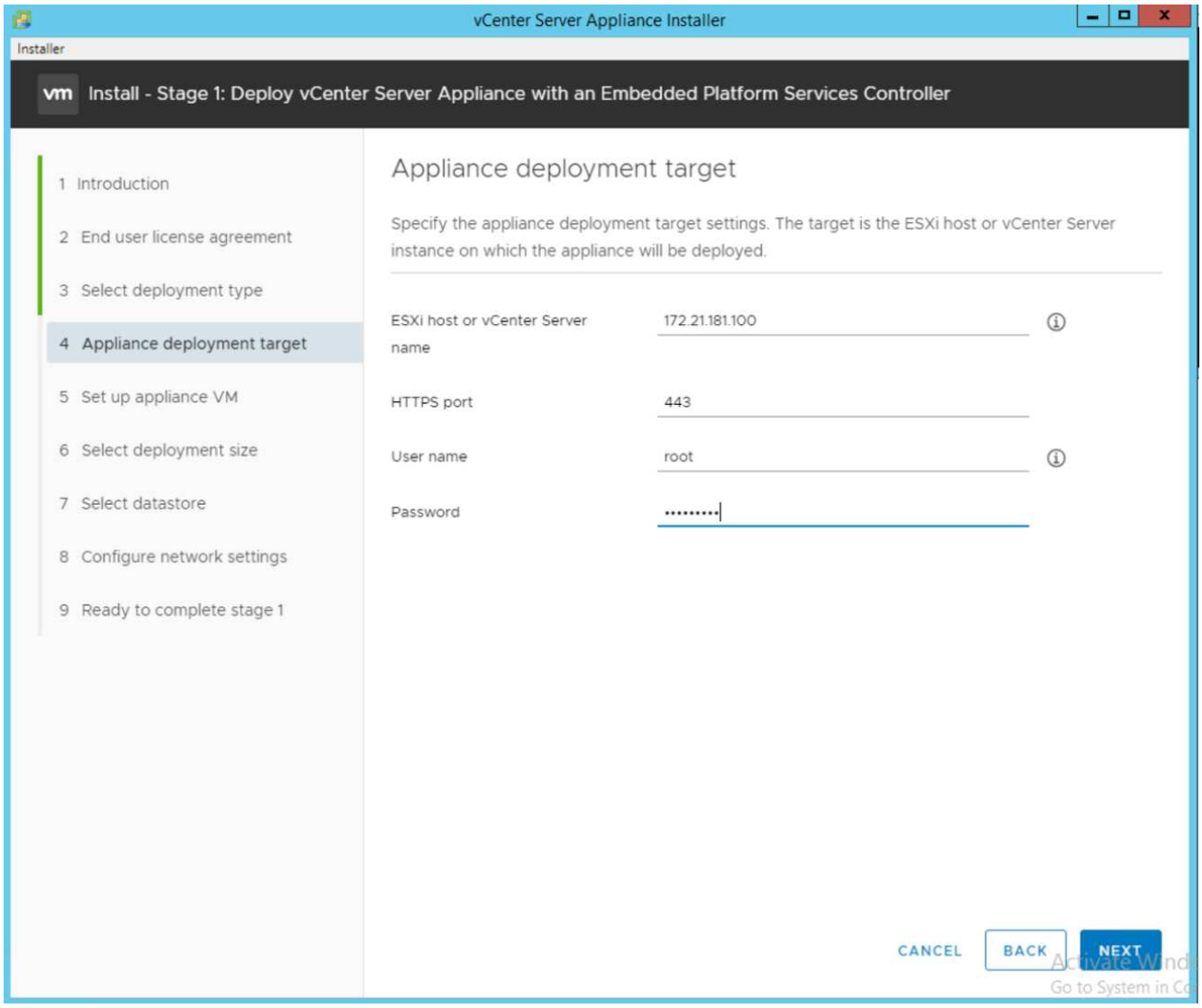


8. 배포 유형으로 임베디드 플랫폼 서비스 컨트롤러 를 선택합니다.

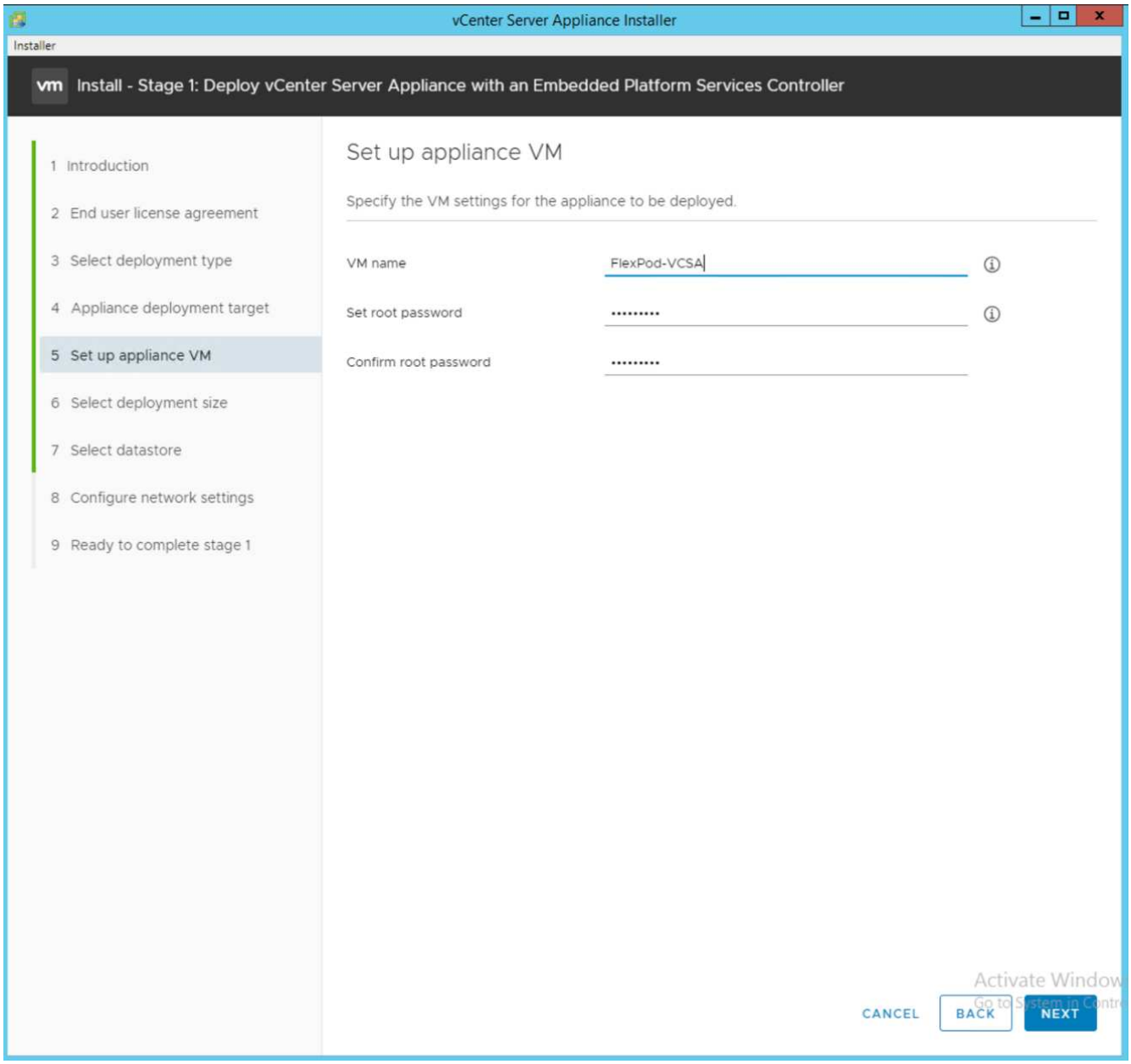


필요한 경우 외부 플랫폼 서비스 컨트롤러 배포도 FlexPod Express 솔루션의 일부로 지원됩니다.

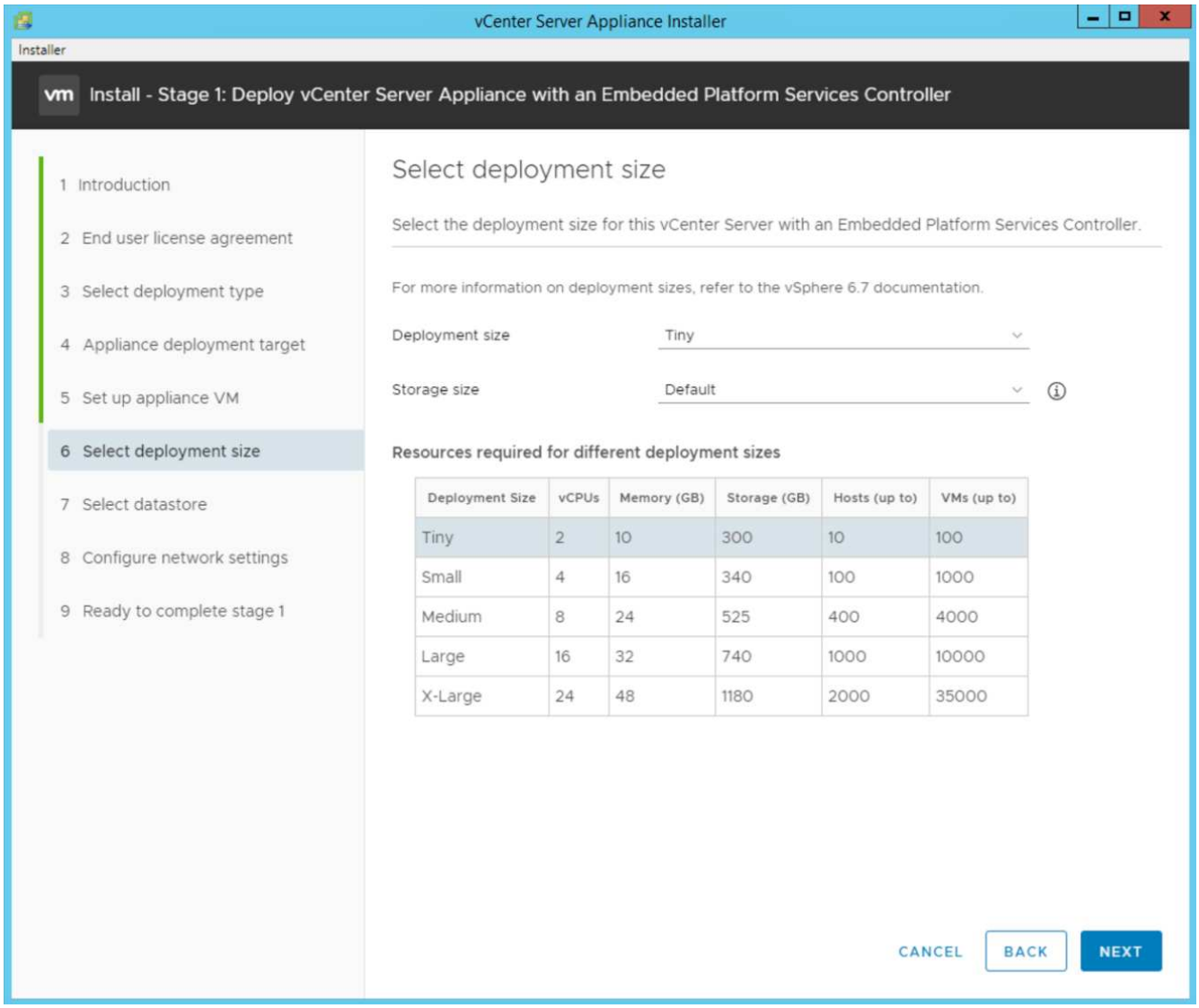
9. 어플라이언스 배포 대상에서 배포한 ESXi 호스트의 IP 주소, 루트 사용자 이름 및 루트 암호를 입력합니다.



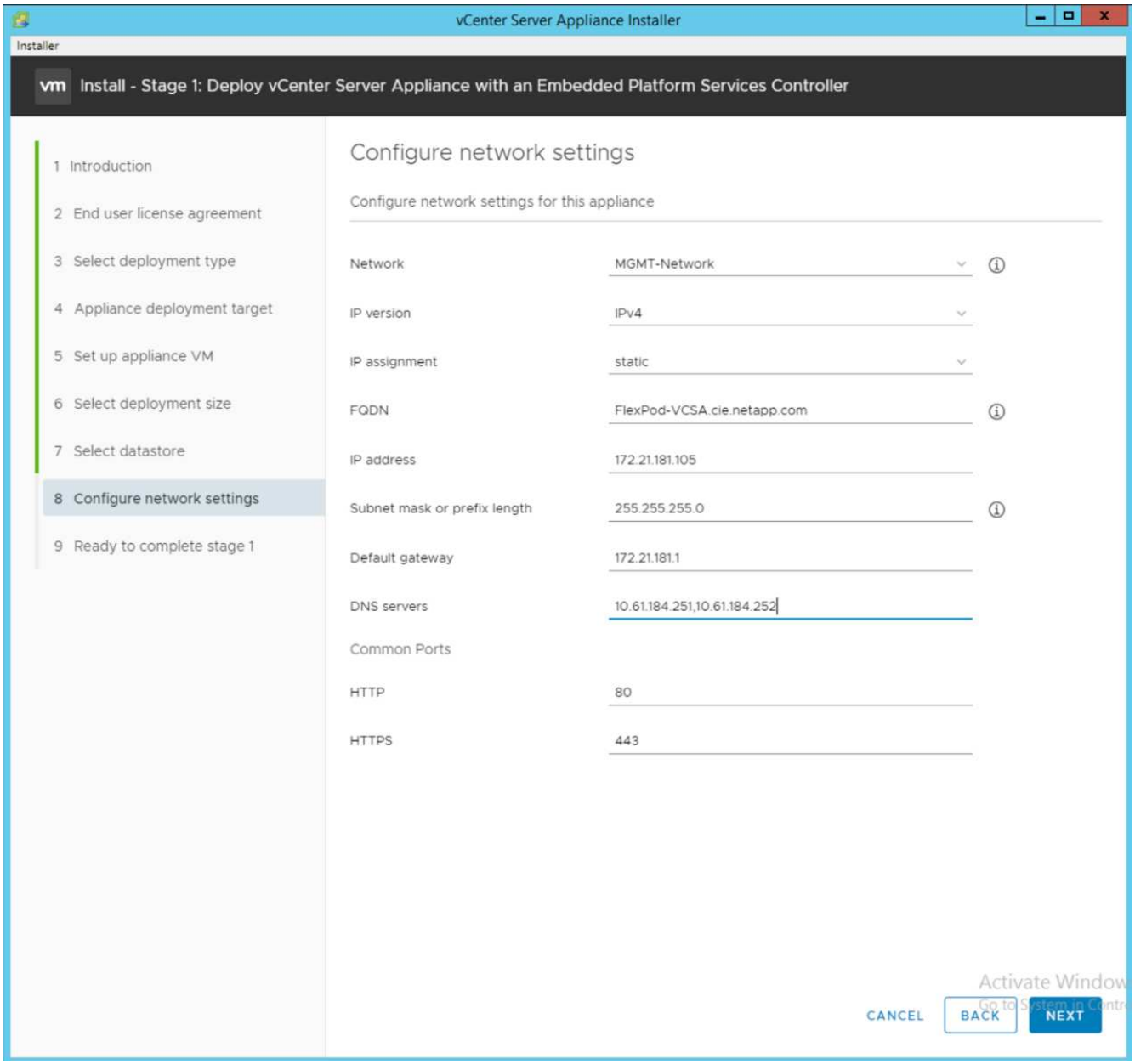
10. VCSA를 VCSA에 사용할 VM 이름 및 루트 암호로 입력하여 어플라이언스 VM을 설정합니다.



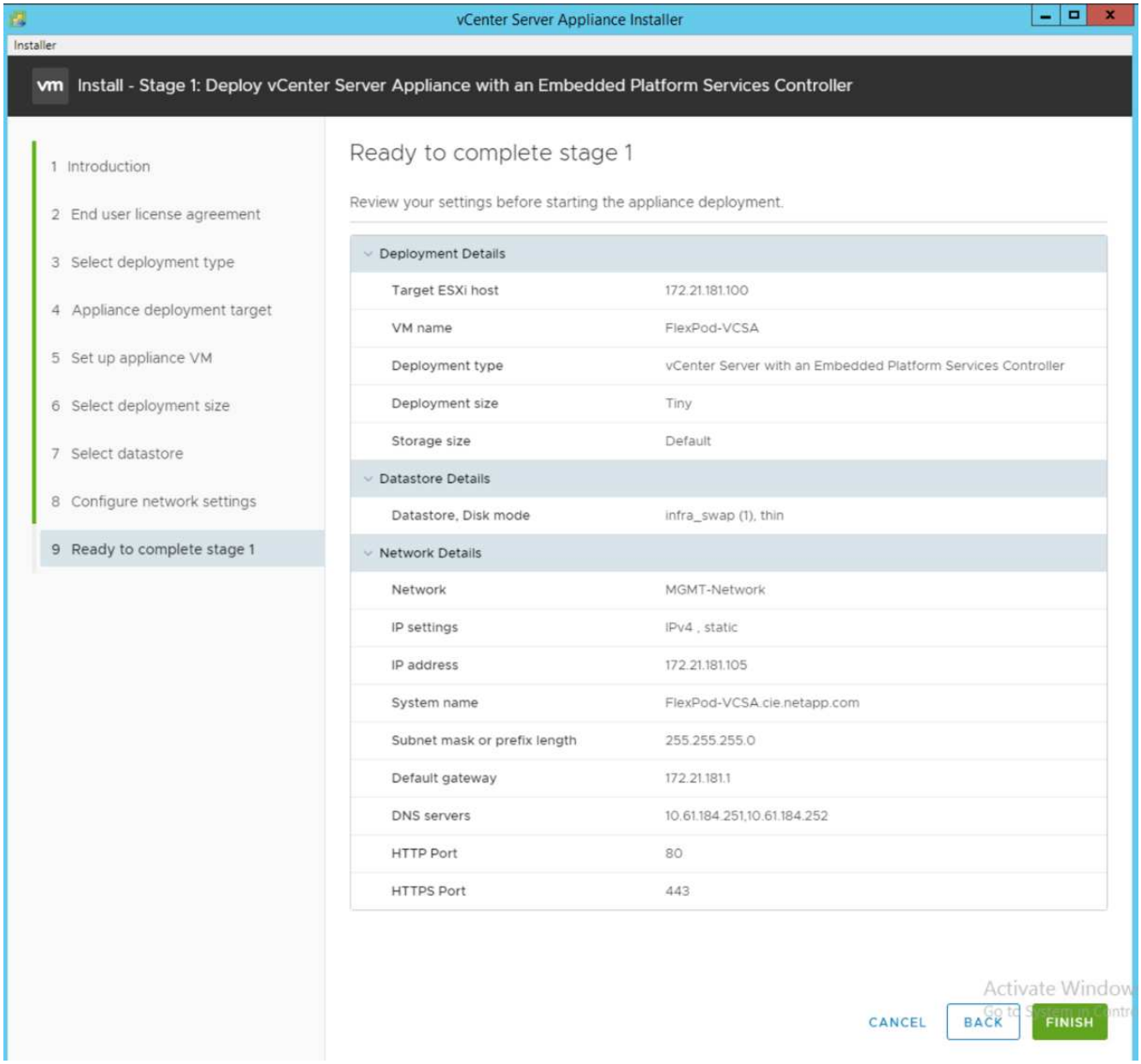
11. 환경에 가장 적합한 구축 크기를 선택합니다. 다음 을 클릭합니다.



12. 'infra_datastore' 데이터 저장소를 선택합니다. 다음 을 클릭합니다.
13. 네트워크 설정 구성 페이지에 다음 정보를 입력하고 다음 을 클릭합니다.
    a. Network 에서 MGMT-Network 를 선택합니다.
    b. VCSA에 사용할 FQDN 또는 IP를 입력합니다.
    c. 사용할 IP 주소를 입력합니다.
    d. 사용할 서브넷 마스크를 입력합니다.
    e. 기본 게이트웨이를 입력합니다.
    f. DNS 서버를 입력합니다.
14. 1단계 완료 준비 페이지에서 입력한 설정이 올바른지 확인합니다. 마침 을 클릭합니다.

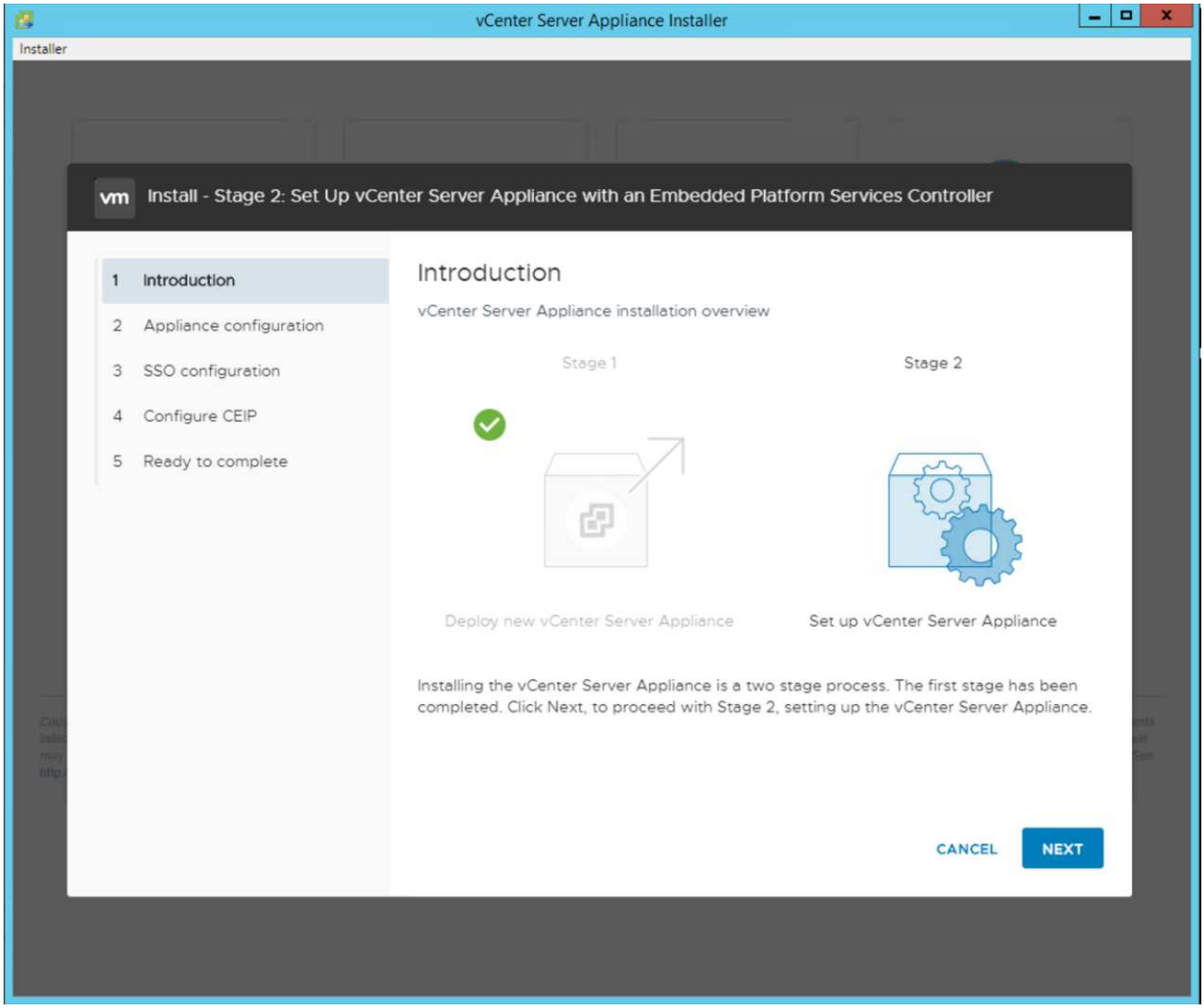


15. 어플라이언스 배포를 시작하기 전에 1단계의 설정을 검토하십시오.

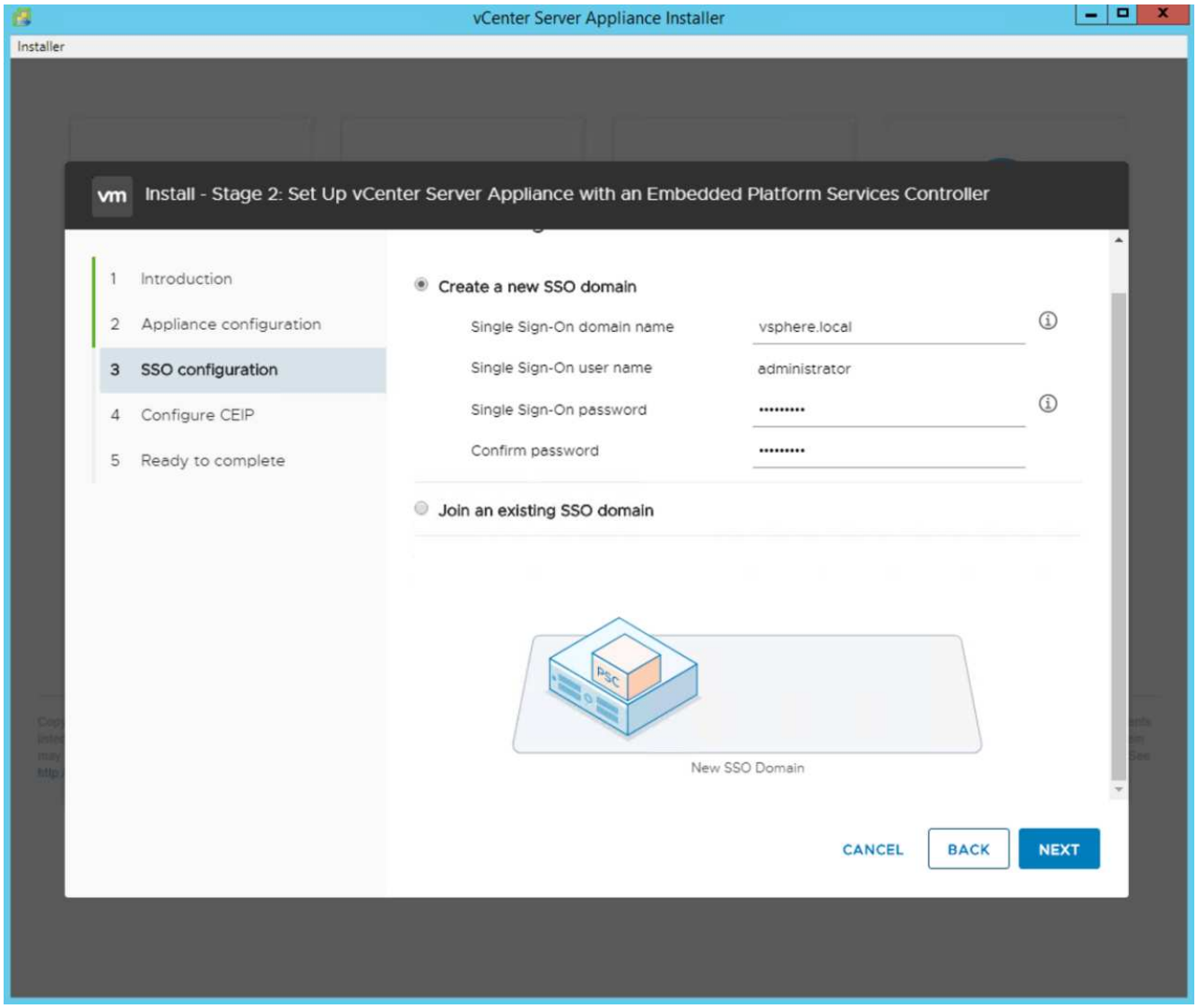


VCSA가 지금 설치됩니다. 이 과정은 몇 분 정도 소요됩니다.

16. 1단계가 완료되면 완료되었다는 메시지가 나타납니다. 계속 을 클릭하여 2단계 구성을 시작합니다.
17. 2단계 소개 페이지에서 다음 을 클릭합니다.

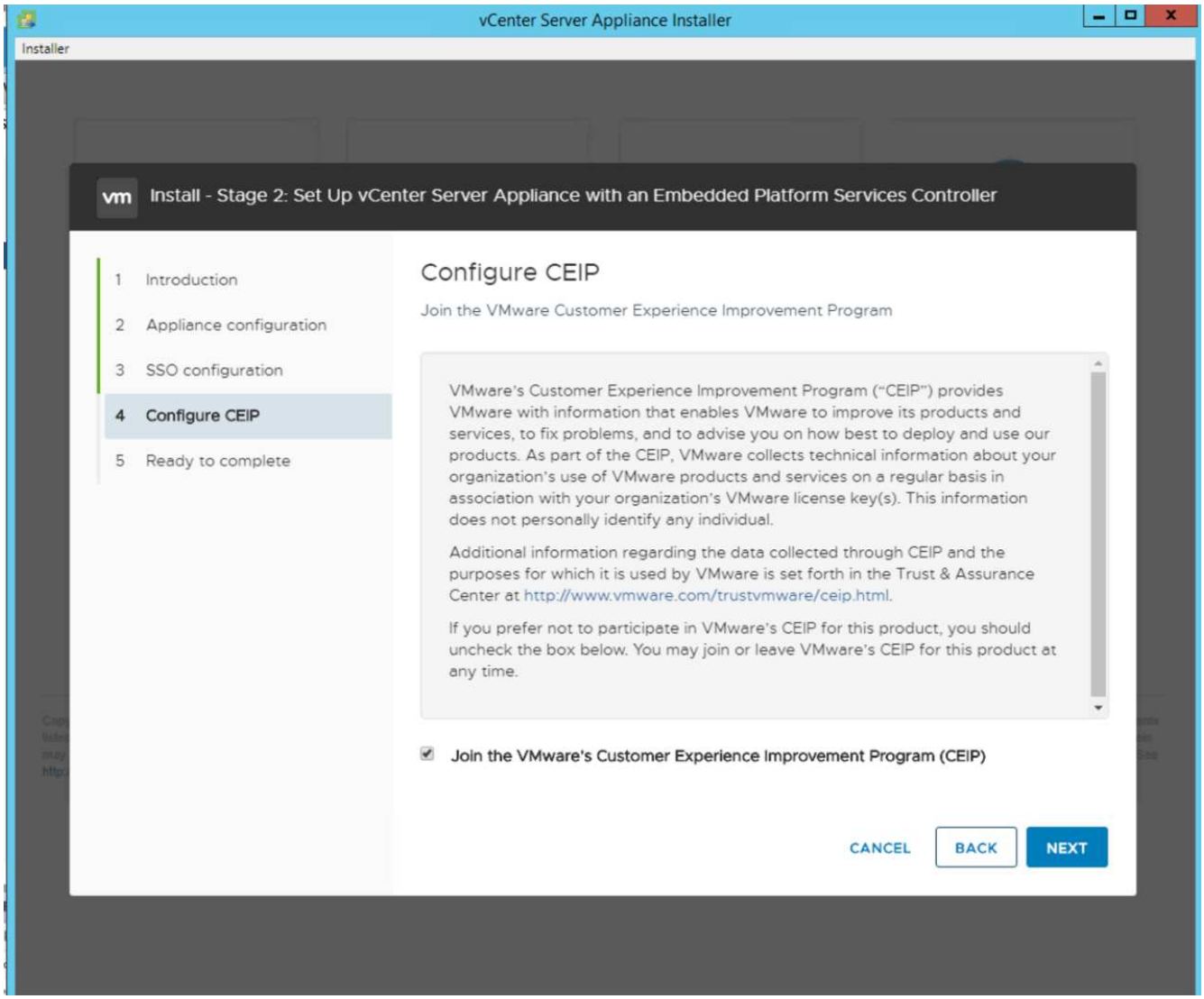


18. NTP 서버 주소에 대해 '<<var_ntp_id>>'를 입력합니다. 여러 NTP IP 주소를 입력할 수 있습니다.
19. vCenter Server HA(고가용성)를 사용하려는 경우 SSH 액세스가 설정되어 있는지 확인합니다.
20. SSO 도메인 이름, 암호 및 사이트 이름을 구성합니다. 다음 을 클릭합니다.

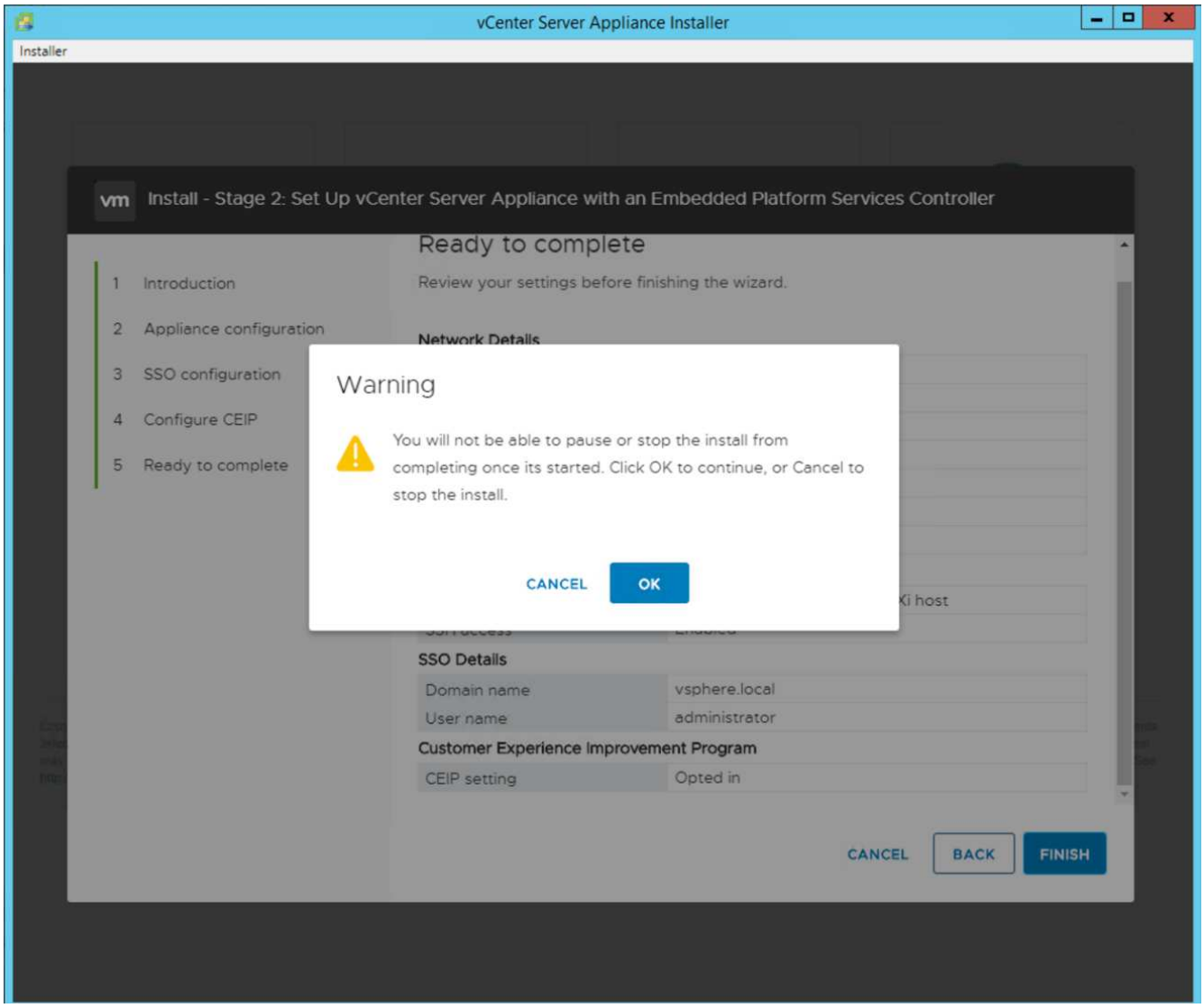


특히 "vsphere.local" 도메인 이름을 벗어나는 경우 이러한 값을 참조로 기록합니다.

21. 원하는 경우 VMware 고객 경험 프로그램에 참여하십시오. 다음 을 클릭합니다.



22. 설정 요약을 봅니다. 마침 을 클릭하거나 뒤로 단추를 사용하여 설정을 편집합니다.
23. 설치가 시작된 후 설치를 일시 중지하거나 중지할 수 없다는 메시지가 나타납니다. 계속하려면 확인을 클릭하십시오.



어플라이언스 설정이 계속됩니다. 이 작업은 몇 분 정도 걸립니다.

설정이 성공했음을 나타내는 메시지가 나타납니다.

24. vCenter Server에 액세스하기 위해 설치 관리자가 제공하는 링크를 클릭할 수 있습니다.

"다음: VMware vCenter Server 6.7U2 및 vSphere 클러스터링 구성"

VMware vCenter Server 6.7U2 및 **vSphere** 클러스터링 구성

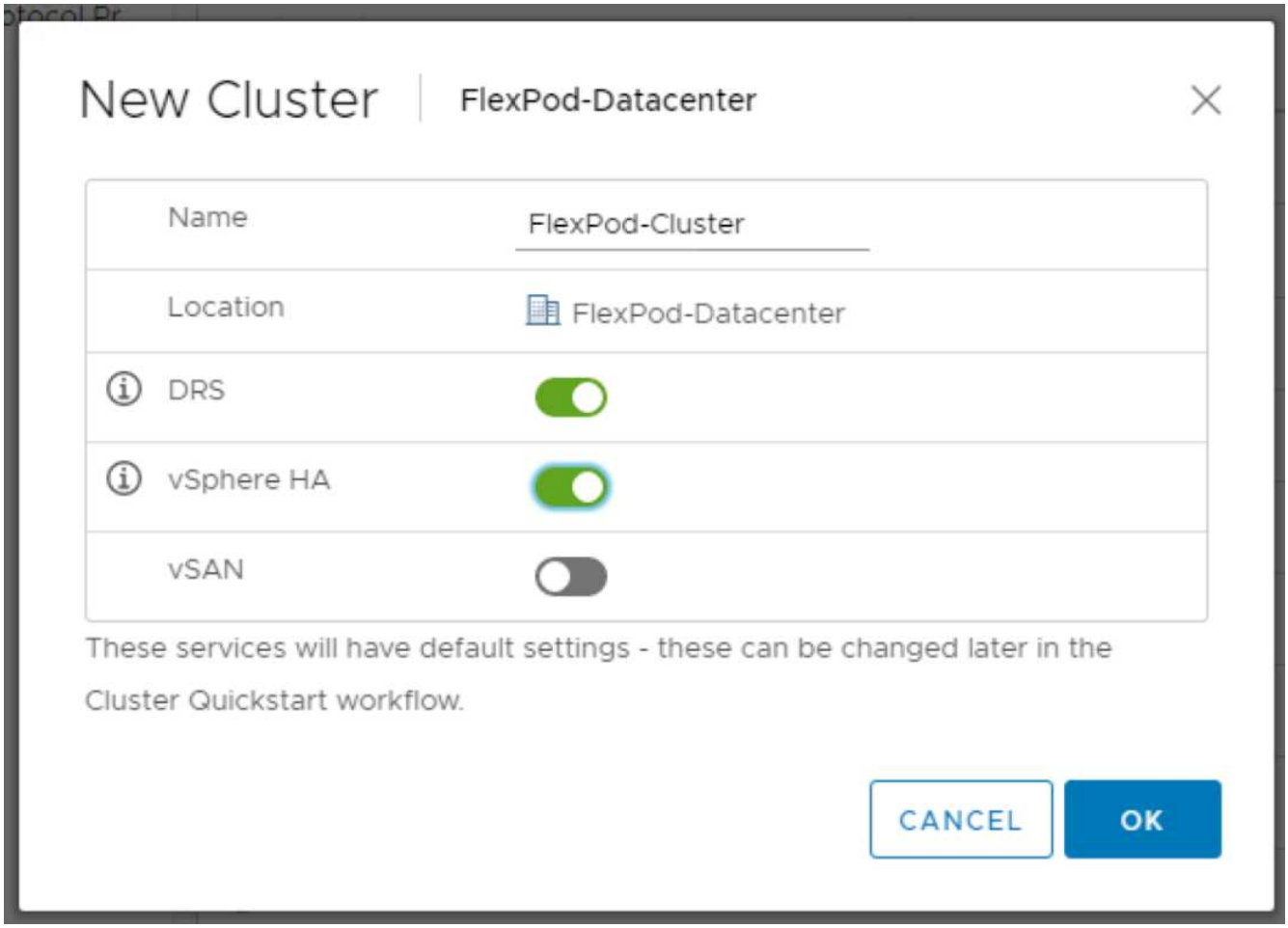
VMware vCenter Server 6.7 및 vSphere 클러스터링을 구성하려면 다음 단계를 수행하십시오.

1. "https://<<FQDN 또는 vCenter의 IP>>/vSphere-client/"로 이동합니다.
2. vSphere Client 시작 을 클릭합니다.
3. 사용자 이름 mailto:administrator@vspehre.loca l [administrator^]@vSphere.local과 VCSA 설정 프로세스 중에 입력한 SSO 암호를 사용하여 로그인합니다.
4. vCenter 이름을 마우스 오른쪽 버튼으로 클릭하고 New Datacenter를 선택합니다.
5. 데이터 센터의 이름을 입력하고 확인 을 클릭합니다.

vSphere 클러스터를 생성합니다

vSphere 클러스터를 생성하려면 다음 단계를 수행하십시오.

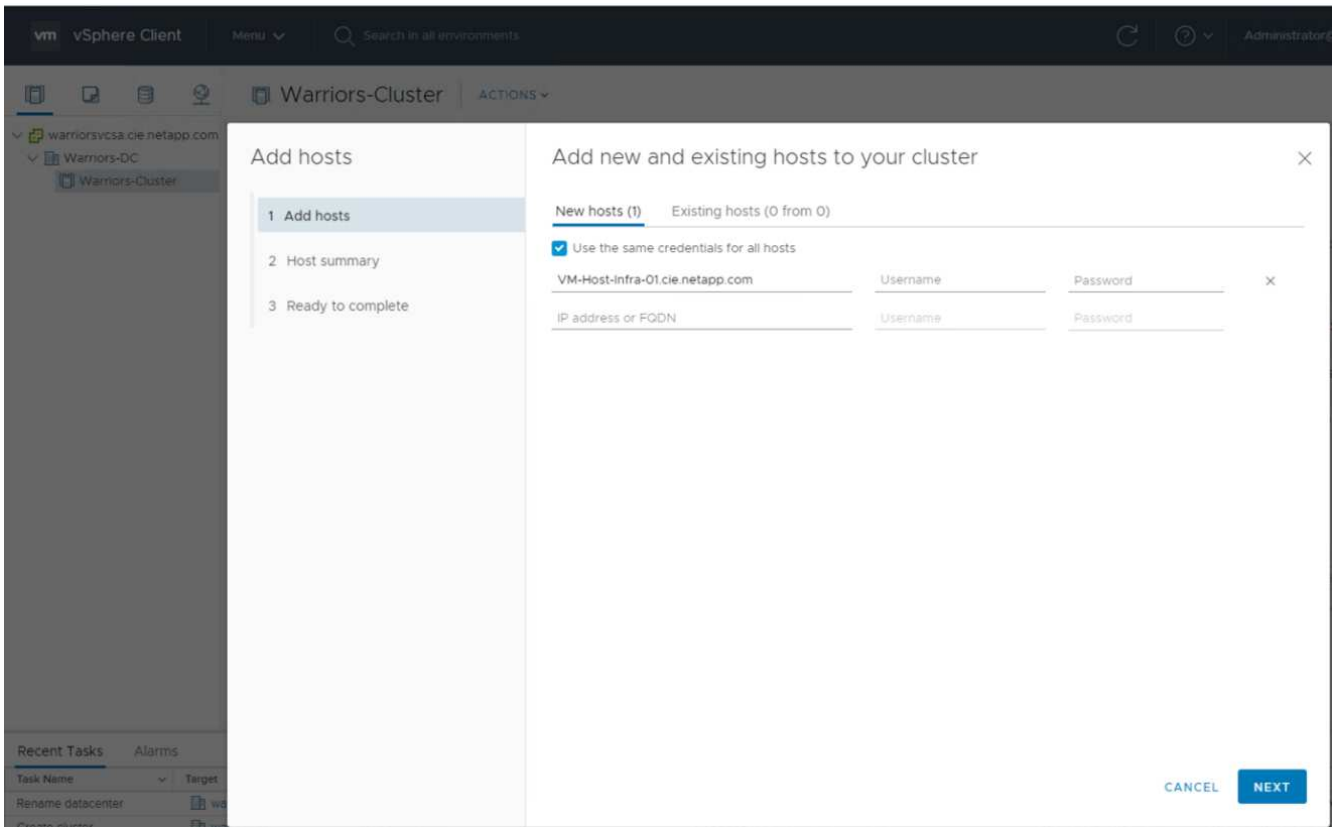
1. 새로 생성된 데이터 센터를 마우스 오른쪽 버튼으로 클릭하고 New Cluster를 선택합니다.
2. 클러스터의 이름을 입력합니다.
3. 확인란을 선택하여 DR 및 vSphere HA를 설정합니다.
4. 확인 을 클릭합니다.



클러스터에 ESXi 호스트를 추가합니다

클러스터에 ESXi 호스트를 추가하려면 다음 단계를 수행하십시오.

1. 클러스터를 마우스 오른쪽 버튼으로 클릭하고 Add Host를 선택합니다.



2. 클러스터에 ESXi 호스트를 추가하려면 다음 단계를 수행하십시오.
   a. 호스트의 IP 또는 FQDN을 입력합니다. 다음 을 클릭합니다.
   b. 루트 사용자 이름과 암호를 입력합니다. 다음 을 클릭합니다.
   c. 예를 클릭하여 호스트의 인증서를 VMware 인증서 서버에서 서명한 인증서로 바꿉니다.
   d. 호스트 요약 페이지에서 다음 을 클릭합니다.
   e. 녹색 + 아이콘을 클릭하여 vSphere 호스트에 라이센스를 추가합니다.
3. 이 단계는 원할 경우 나중에 완료할 수 있습니다.
   a. 다음 을 클릭하여 잠금 모드를 해제합니다.
   b. VM 위치 페이지에서 다음 을 클릭합니다.
   c. 완료 준비 페이지를 검토합니다. 뒤로 단추를 사용하여 변경하거나 마침 을 선택합니다.
4. Cisco UCS 호스트 B에 대해 1단계와 2단계를 반복합니다

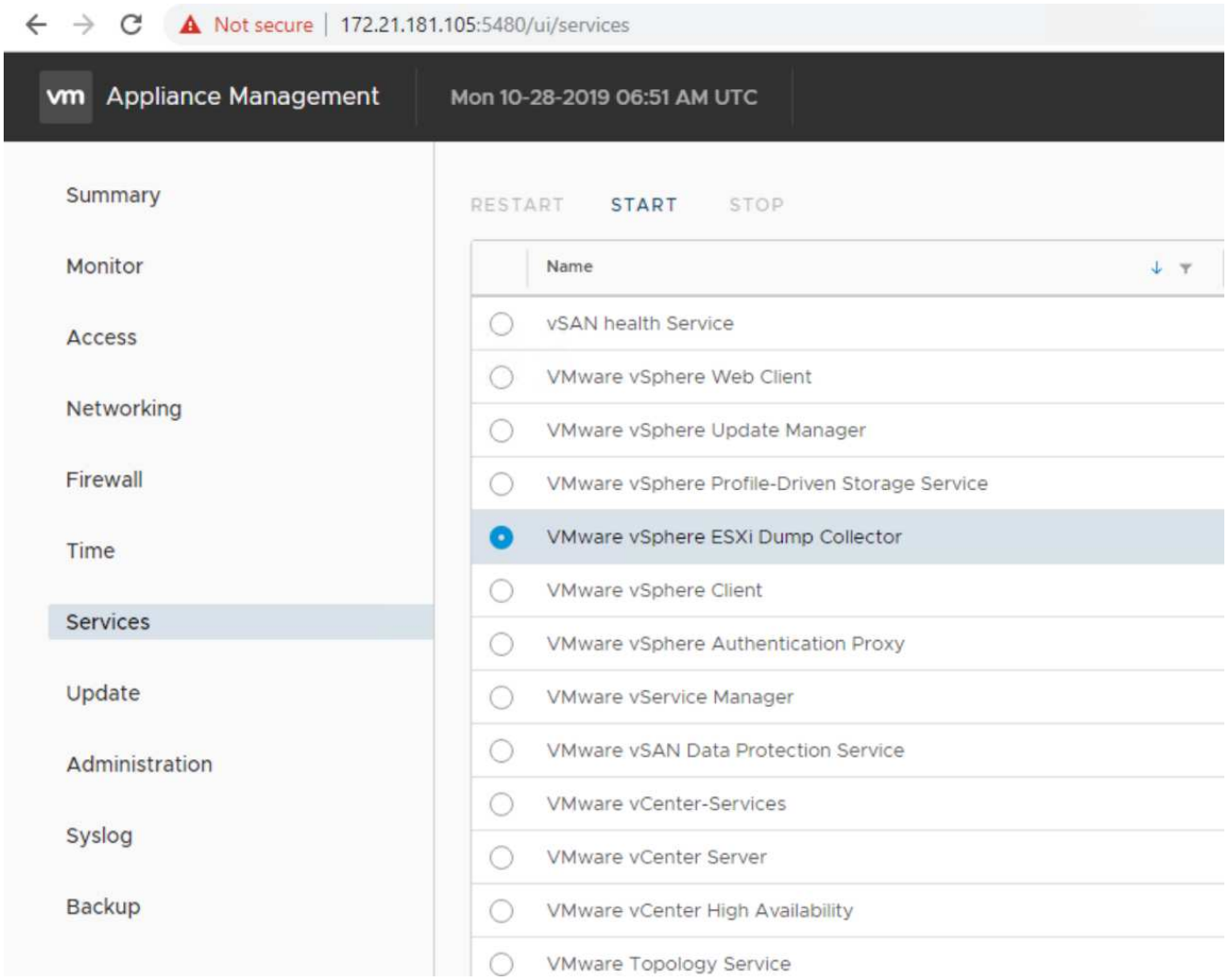
> FlexPod Express 구성에 추가된 모든 호스트에 대해 이 프로세스를 완료해야 합니다.

ESXi 호스트에서 코어 덤프를 구성합니다

ESXi 호스트에서 코어 덤프를 구성하려면 다음 단계를 수행하십시오.

1. https:// 에 로그인합니다 "vCenter 를 참조하십시오" IP: 5480/, 사용자 이름으로 root를 입력하고 루트 암호를 입력합니다.
2. 서비스를 클릭하고 VMware vSphere ESXi Dump Collector를 선택합니다.

3. VMware vSphere ESXi Dump Collector 서비스를 시작합니다.



4. SSH를 사용하여 관리 IP ESXi 호스트에 연결하고 사용자 이름에 root를 입력한 다음 루트 암호를 입력합니다.
5. 다음 명령을 실행합니다.

```
esxcli system coredump network set -i ip_address_of_core_dump_collector
-v vmk0 -o 6500
esxcli system coredump network set --enable=true
esxcli system coredump network check
```

6. 최종 명령어를 입력하면 확인된 netdump server가 실행 중인 것으로 확인되었다는 메시지가 나타난다.

```
root@VM-Host-Infra-01:~] esxcli system coredump network set -i 172.21.181.105 -
 vmk0 -o 6500
root@VM-Host-Infra-01:~]
root@VM-Host-Infra-01:~] esxcli system coredump network set --enable=true
root@VM-Host-Infra-01:~] esxcli system coredump network check
erified the configured netdump server is running
```

FlexPod Express에 추가된 모든 호스트에 대해 이 프로세스를 완료해야 합니다.

이 검증에서 "ip_address_of_core_dump_collector"는 vCenter IP입니다.

"다음: NetApp Virtual Storage Console 9.6 구축 절차"

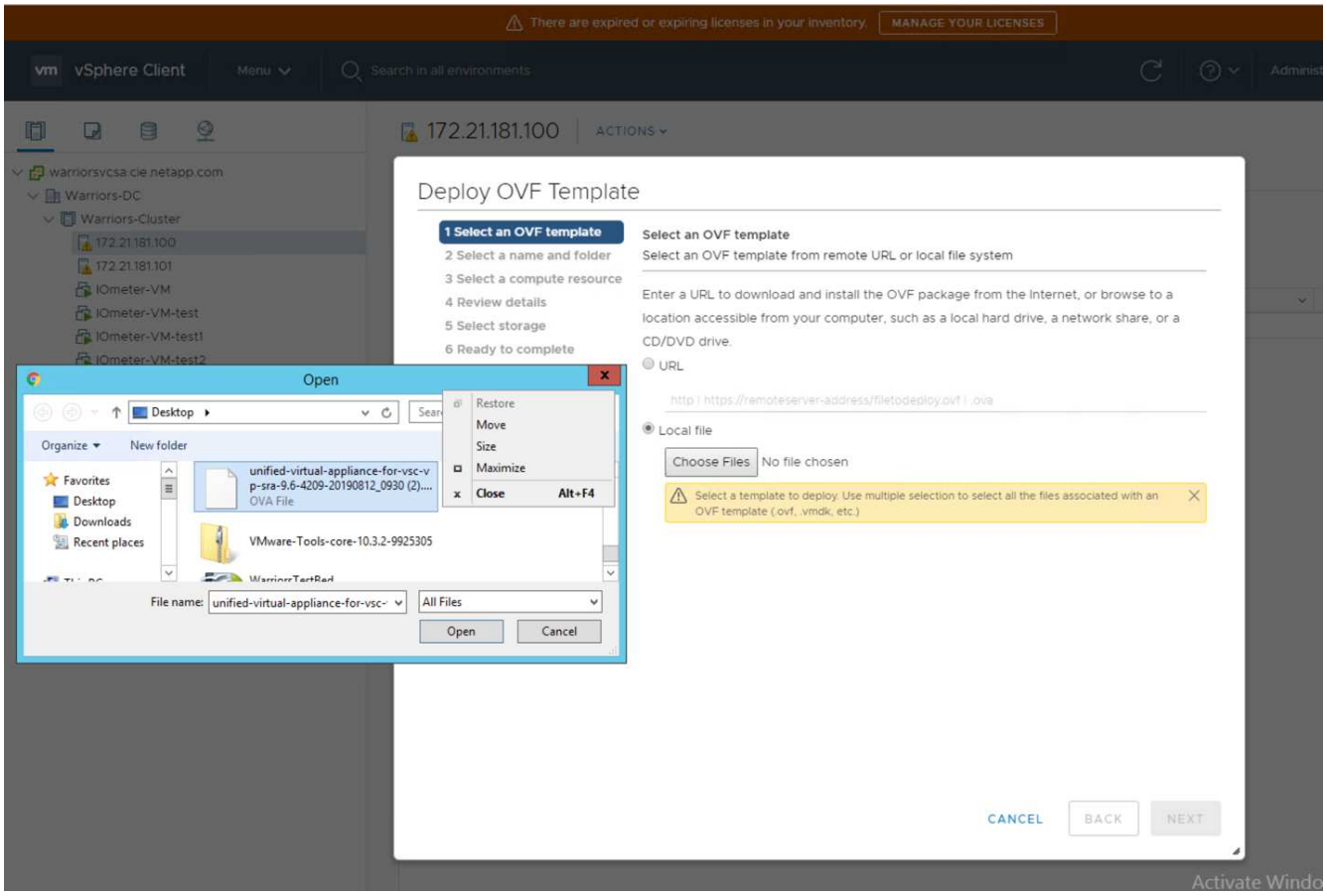
NetApp Virtual Storage Console 9.6 구축 절차

이 섹션에서는 NetApp VSC(가상 스토리지 콘솔)의 구축 절차를 설명합니다.

Virtual Storage Console 9.6을 설치합니다

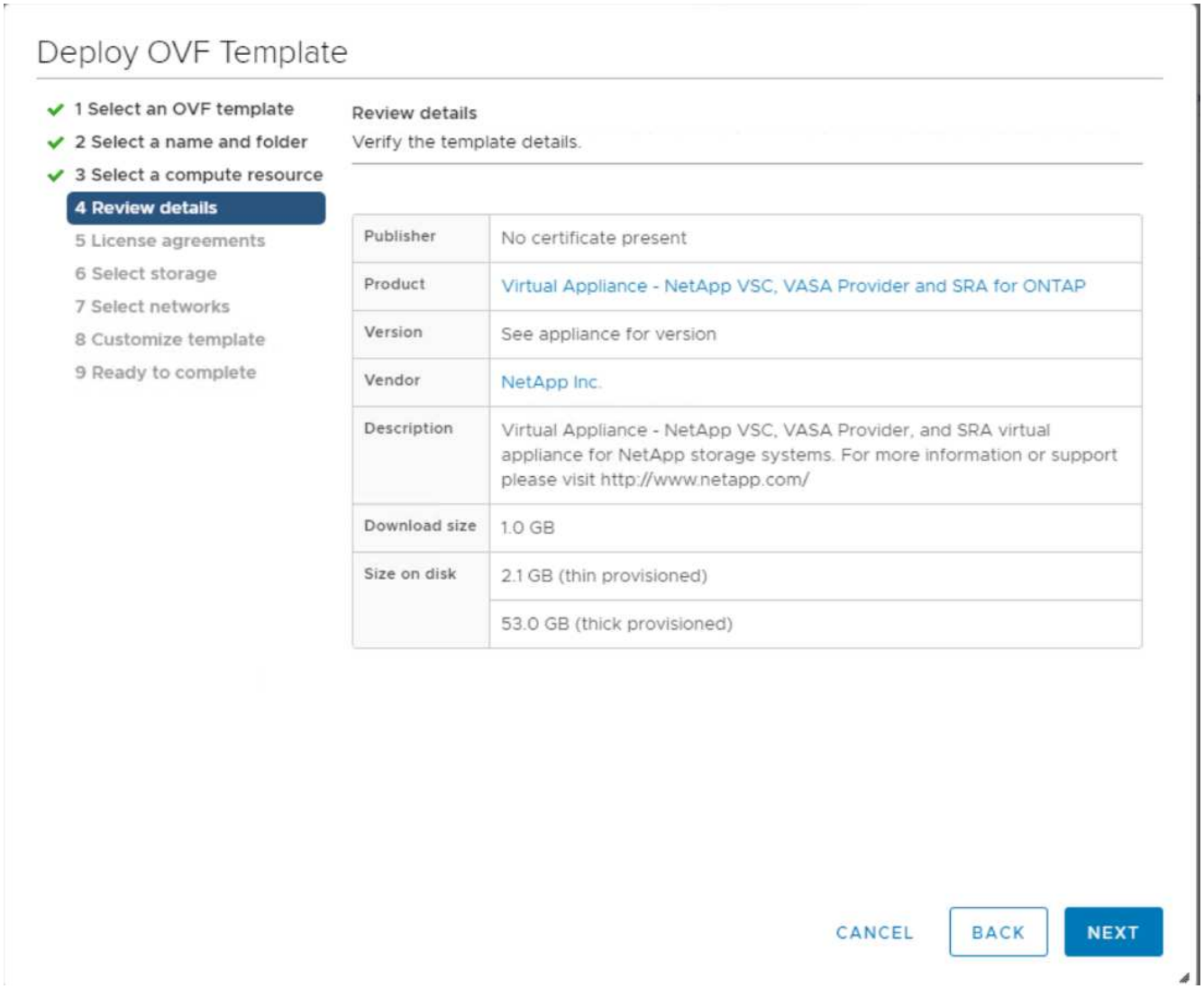
OVF(Open Virtualization Format) 배포를 사용하여 VSC 9.6 소프트웨어를 설치하려면 다음 단계를 수행하십시오.

1. vSphere Web Client > Host Cluster > Deploy OVF Template 으로 이동합니다.
2. NetApp Support 사이트에서 다운로드한 VSC OVF 파일로 이동합니다.

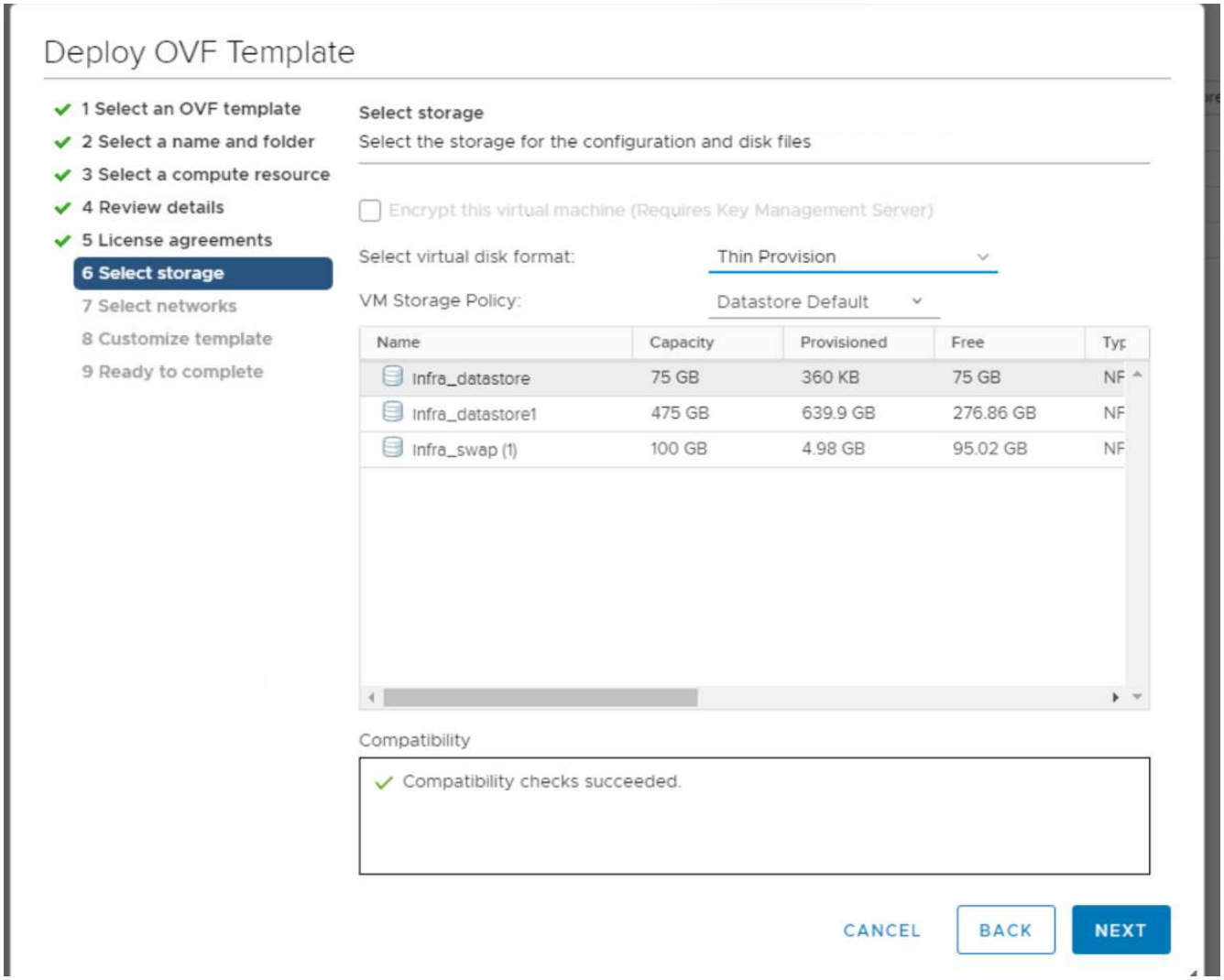


3. VM 이름을 입력하고 배포할 데이터 센터 또는 폴더를 선택합니다. 다음 을 클릭합니다.

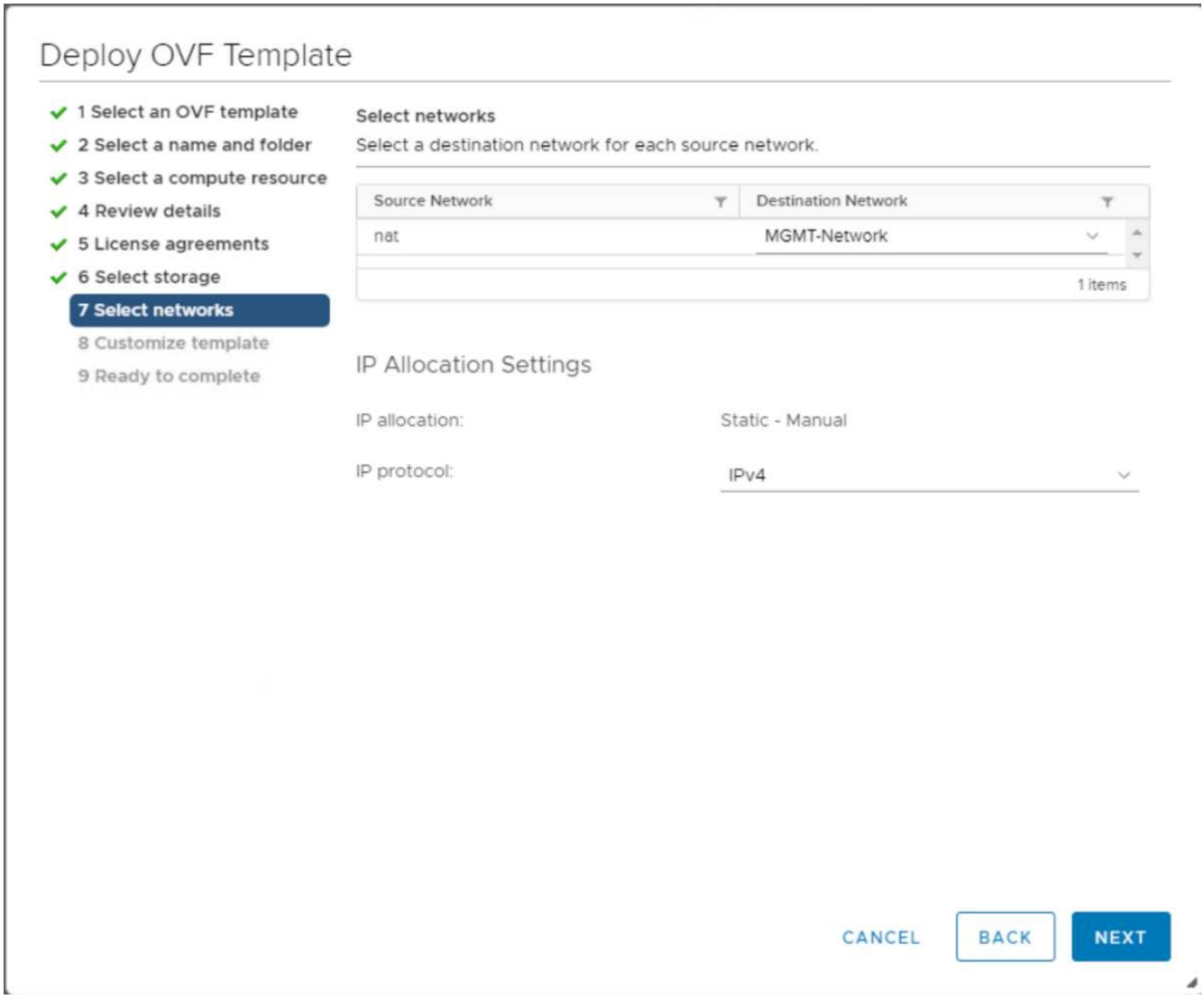
4. FlexPod-Cluster ESXi 클러스터를 선택하고 Next를 클릭합니다.
5. 세부 정보를 검토하고 Next를 클릭합니다.



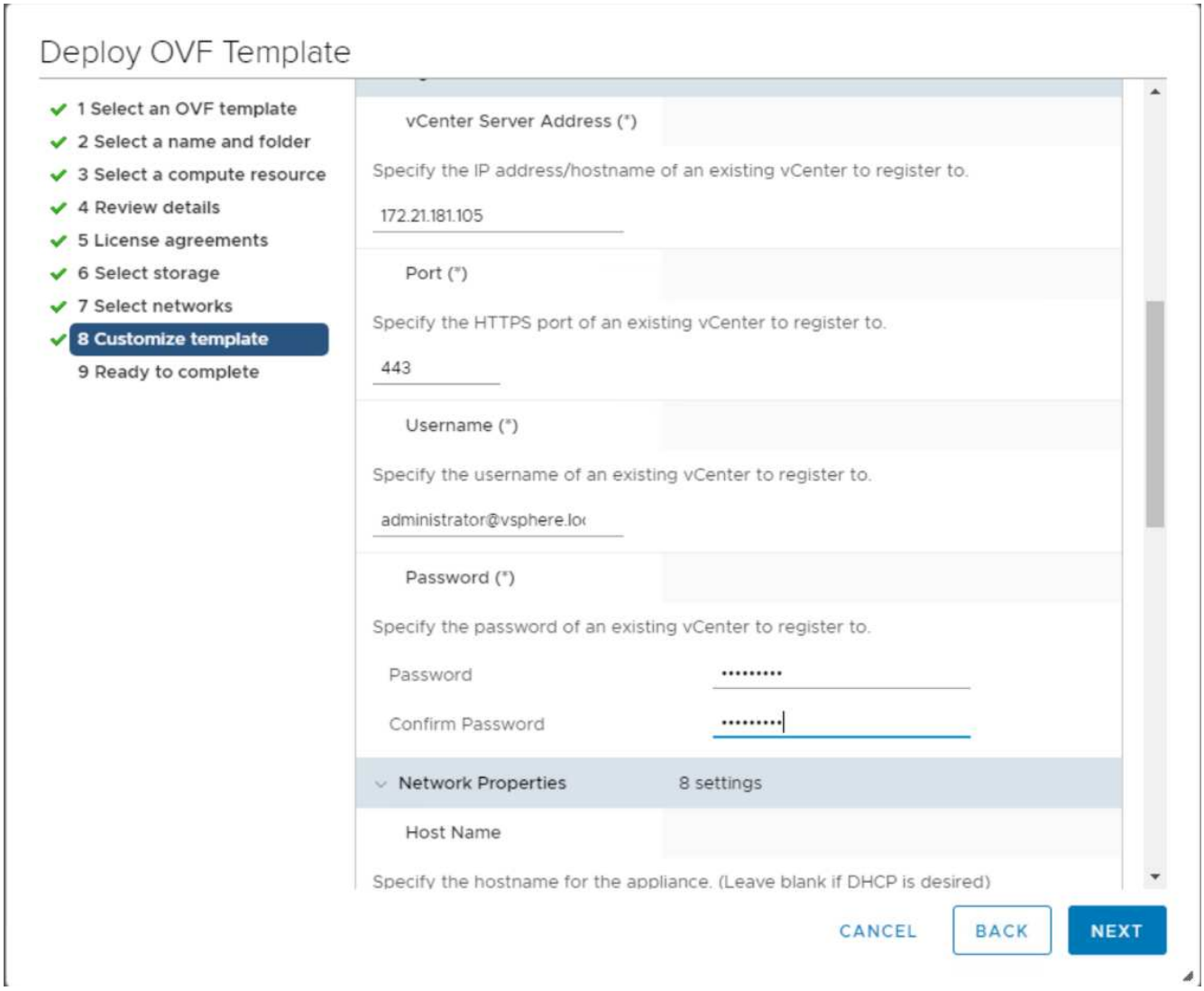
6. Accept(수락) 를 클릭하여 라이센스를 수락하고 Next(다음) 를 클릭합니다.
7. Thin Provision 가상 디스크 형식과 NFS 데이터 저장소 중 하나를 선택합니다. 다음 을 클릭합니다.



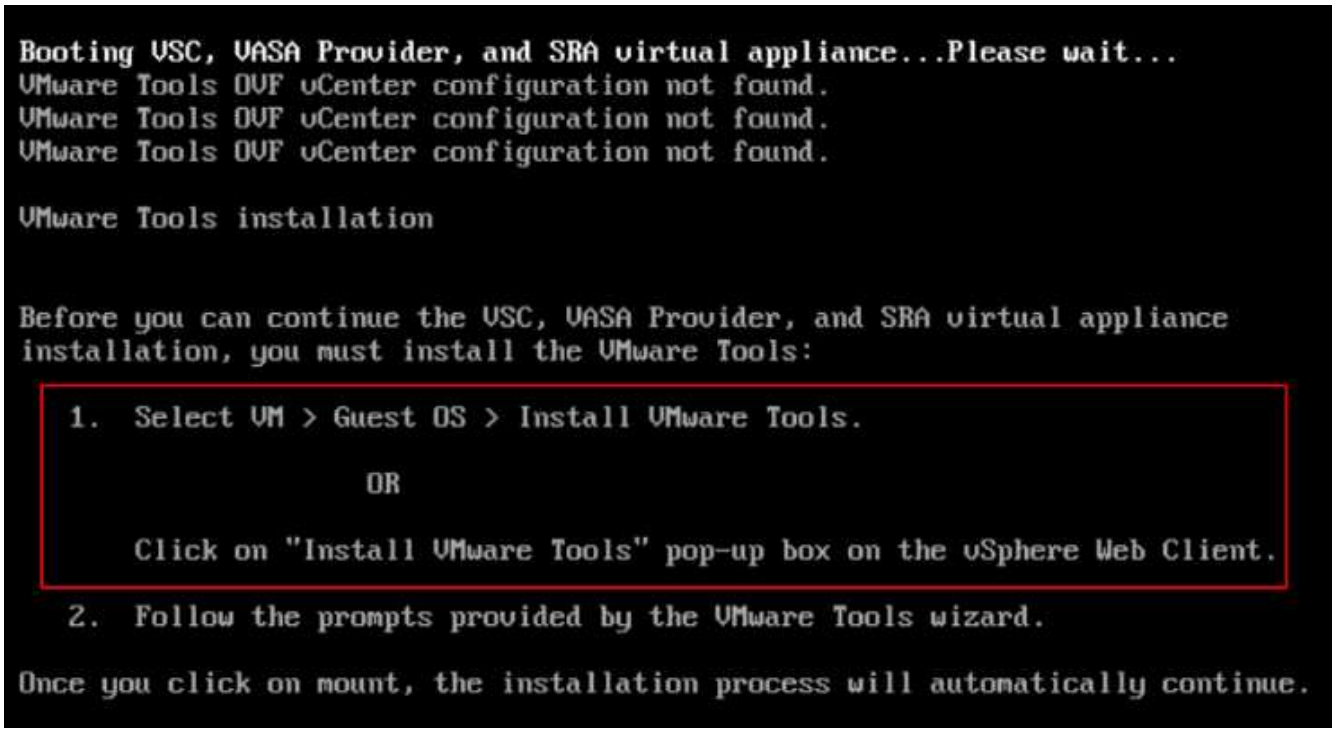
8. 네트워크 선택에서 대상 네트워크를 선택하고 다음을 클릭합니다.



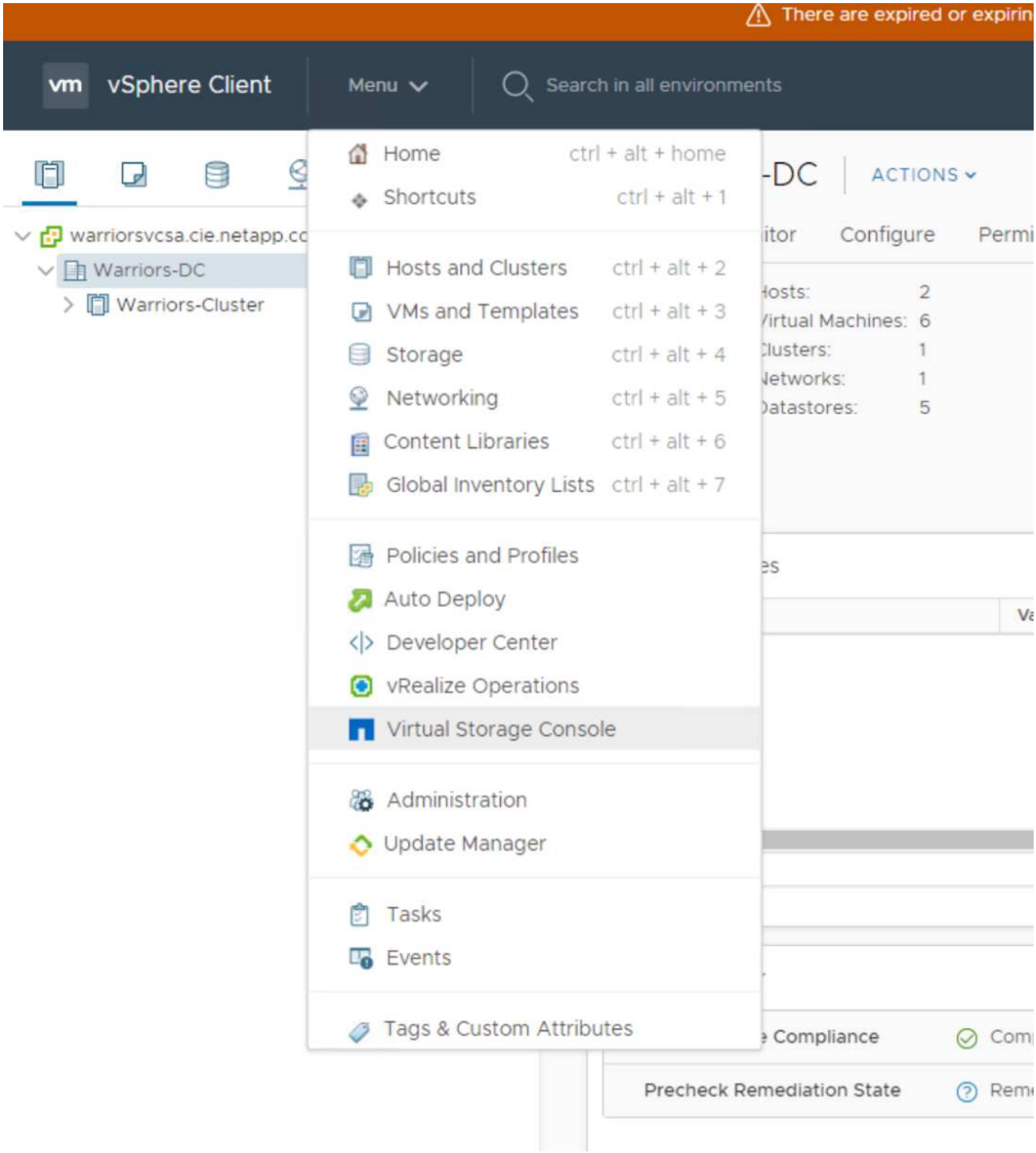
9. 템플릿 사용자 지정에서 VSC 관리자 암호, vCenter 이름 또는 IP 주소, 기타 구성 정보를 입력하고 다음을 클릭합니다.



10. 입력한 구성 세부 정보를 검토하고 Finish를 클릭하여 NetApp-VSC VM 구축을 완료합니다.
11. NetApp-VSC VM의 전원을 켜고 VM 콘솔을 엽니다.
12. NetApp-VSC VM 부팅 프로세스 중에 VMware 툴을 설치하라는 메시지가 표시됩니다. vCenter에서 NetApp-VSC VM > 게스트 OS > VMware 툴 설치 를 선택합니다.



13. OVF 템플릿 사용자 지정 중에 네트워킹 구성 및 vCenter 등록 정보가 제공되었습니다. 따라서 NetApp VSC VM을 실행한 후 VSC, VASA(vSphere API for Storage Awareness), VMware SRA(Storage Replication Adapter)가 vCenter에 등록됩니다.
14. vCenter Client에서 로그아웃하고 다시 로그인합니다. 홈 메뉴에서 NetApp VSC가 설치되었는지 확인합니다.



NetApp NFS VAAI 플러그인을 다운로드하고 설치합니다

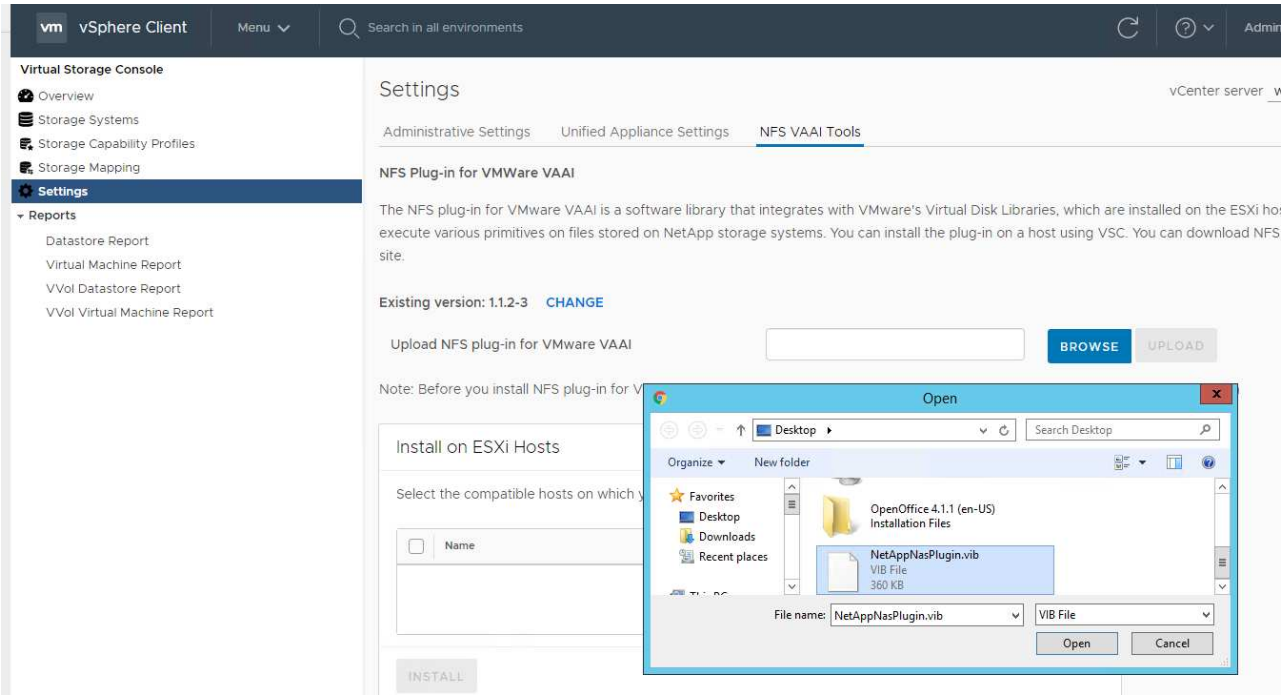
NetApp NFS VAAI 플러그인을 다운로드하고 설치하려면 다음 단계를 완료하십시오.

1. NetApp NFS Plug-in 1.1.2 for VMware를 다운로드합니다. NFS 플러그인 다운로드 페이지에서 VIB' 파일을 로컬 컴퓨터 또는 관리 호스트에 저장합니다.
2. NetApp NFS Plug-in for VMware VAAI 다운로드:
   a. 로 이동합니다 "소프트웨어 다운로드 페이지".

b. 아래로 스크롤하여 VMware VAAI용 NetApp NFS 플러그인 을 클릭합니다.

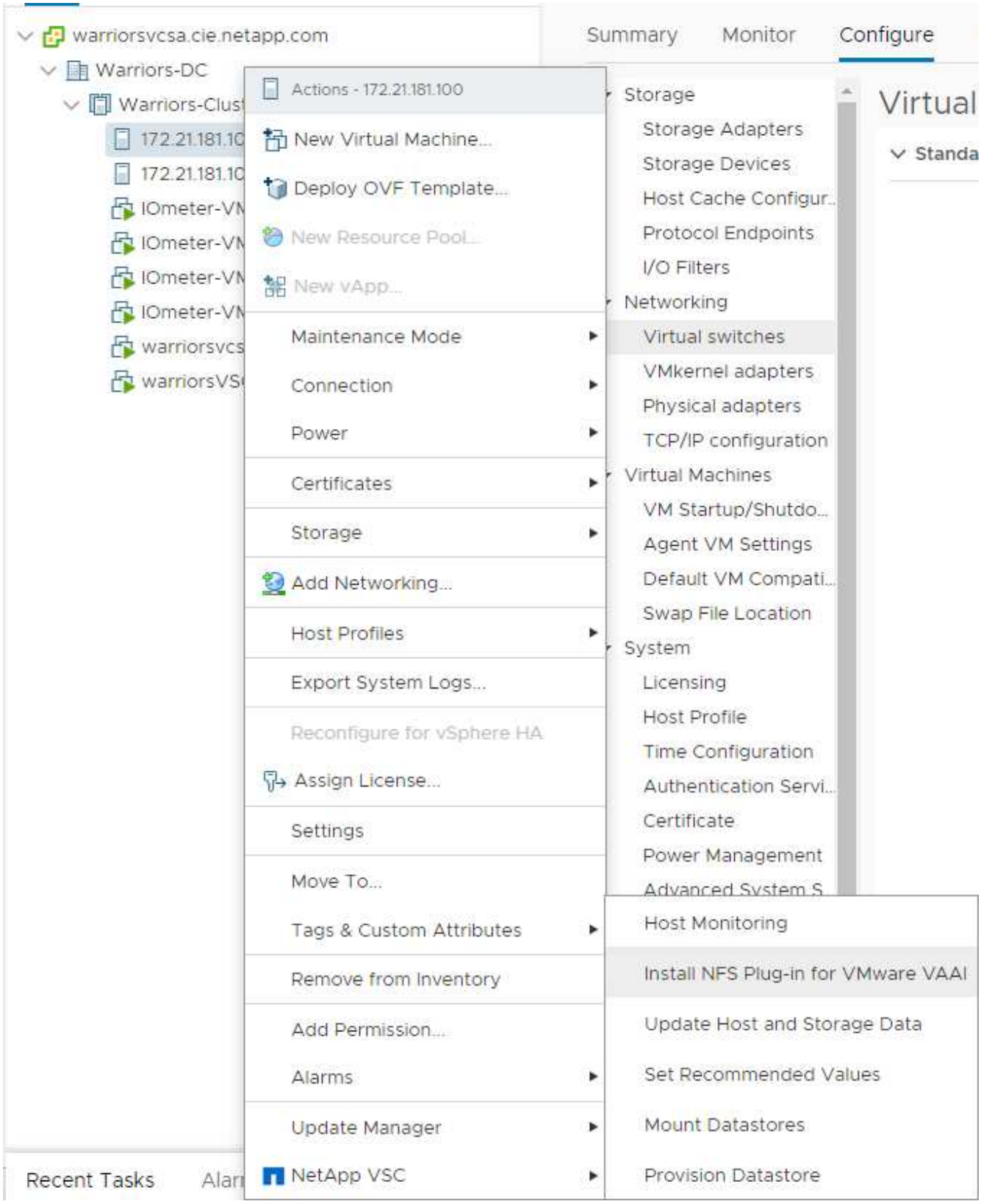
c. vSphere 웹 클라이언트의 홈 화면에서 가상 스토리지 콘솔을 선택합니다.

d. Virtual Storage Console > Settings > NFS VAAI Tools 에서 Select File 을 선택하고 다운로드한 플러그인이 저장된 위치로 이동하여 NFS 플러그인을 업로드합니다.



3. 업로드 를 클릭하여 플러그인을 vCenter로 전송합니다.

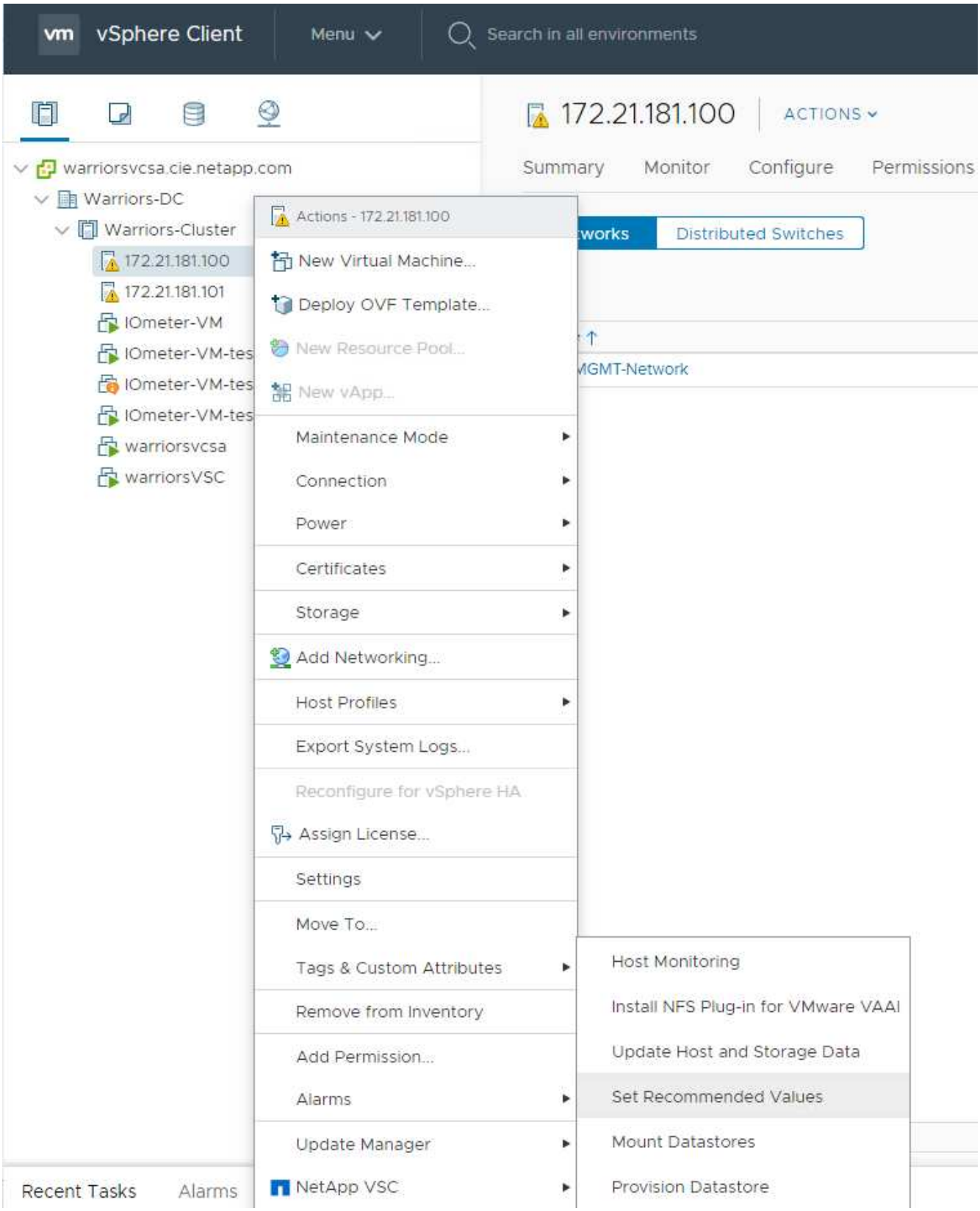
4. 호스트를 선택한 다음 NetApp VSC > Install NFS Plug-in for VMware VAAI 를 선택합니다.



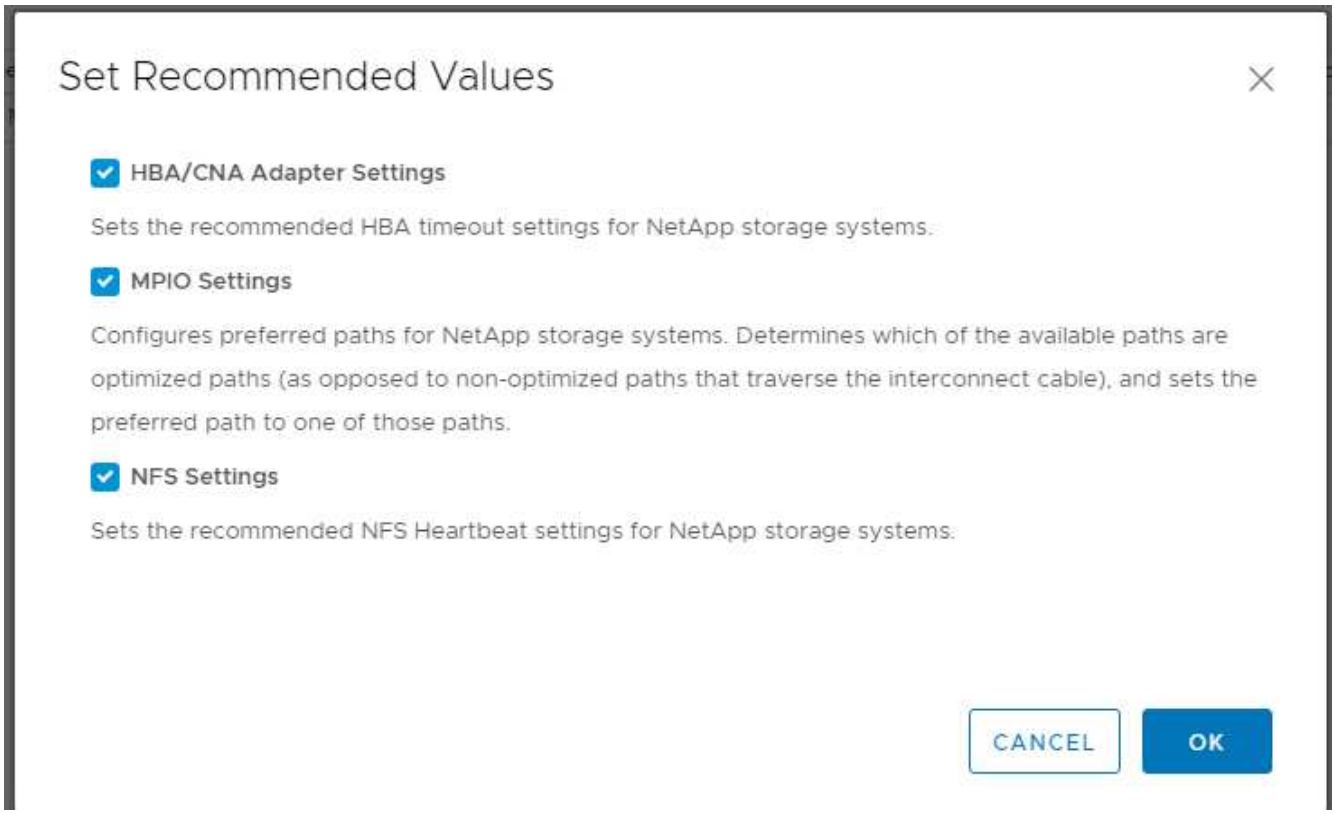
ESXi 호스트에 대한 최적의 스토리지 설정을 사용합니다

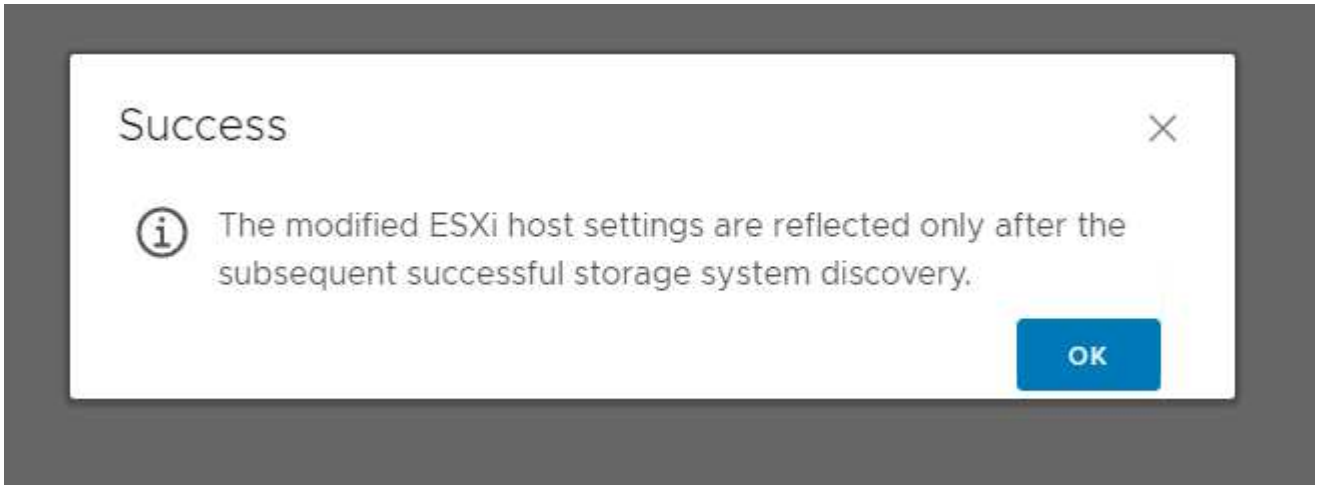
VSC를 사용하면 NetApp 스토리지 컨트롤러에 연결된 모든 ESXi 호스트의 스토리지 관련 설정을 자동으로 구성할 수 있습니다. 이러한 설정을 사용하려면 다음 단계를 완료하십시오.

1. 홈 화면에서 vCenter > 호스트 및 클러스터 를 선택합니다. 각 ESXi 호스트에 대해 NetApp VSC > Set Recommended Values를 마우스 오른쪽 버튼으로 클릭하고 선택합니다.



2. 선택한 vSphere 호스트에 적용할 설정을 선택합니다. 확인 을 클릭하여 설정을 적용합니다.





3. 이러한 설정을 적용한 후 ESXi 호스트를 재부팅합니다.

결론

FlexPod Express는 업계 최고의 구성요소를 사용하는 검증된 설계를 통해 간단하고 효율적인 솔루션을 제공합니다. 구성요소 추가를 통해 확장하여 특정 비즈니스 요구에 맞게 FlexPod Express를 조정할 수 있습니다. FlexPod Express는 전용 솔루션이 필요한 중소기업, ROBO 및 기타 기업을 위해 설계되었습니다.

감사의 말

저자는 John George가 이 설계에 대한 지원과 기여에 대해 인정하기를 원합니다.

추가 정보를 찾을 수 있는 위치

이 문서에 설명된 정보에 대한 자세한 내용은 다음 문서 및/또는 웹 사이트를 참조하십시오.

NetApp 제품 설명서

http://docs. "넷엡"com

FlexPod Express with Guide를 참조하십시오

NVA-1139-design:FlexPod Express with Cisco UCS C-Series 및 NetApp AFF C190 Series

"https://www.netapp.com/us/media/nva-1139-design.pdf"

버전 기록

버전	날짜	문서 버전 기록
버전 1.0	2019년 11월	최초 릴리스.

FlexPod Express with Cisco UCS C-Series and AFF A220 Series 설계 가이드 를 참조하십시오

NVA-1125-design: FlexPod Express with Cisco UCS C-Series and AFF A220 Series

Savita Kumari, NetApp과의 파트너십:

업계 동향에 따르면 많은 데이터 센터가 공유 인프라 및 클라우드 컴퓨팅으로 전환하고 있습니다. 또한 기업에서는 데이터 센터에서 친숙한 기술을 활용하여 원격 사무소 및 지사를 위한 간편하고 효율적인 솔루션을 찾고 있습니다.

FlexPod Express는 Cisco UCS(Cisco Unified Computing System), Cisco Nexus 스위치 제품군, NetApp AFF를 기반으로 사전 설계되고 모범 사례 데이터 센터 아키텍처입니다. FlexPod Express의 구성 요소는 FlexPod 데이터 센터 구성 요소와 비슷하므로 더 작은 규모로 전체 IT 인프라 환경에서 관리 시너지 효과를 실현할 수 있습니다. FlexPod 데이터 센터 및 FlexPod 익스프레스는 가상화 및 베어 메탈 운영 체제 및 엔터프라이즈 워크로드를 위한 최적의 플랫폼입니다.

"다음: 프로그램 요약."

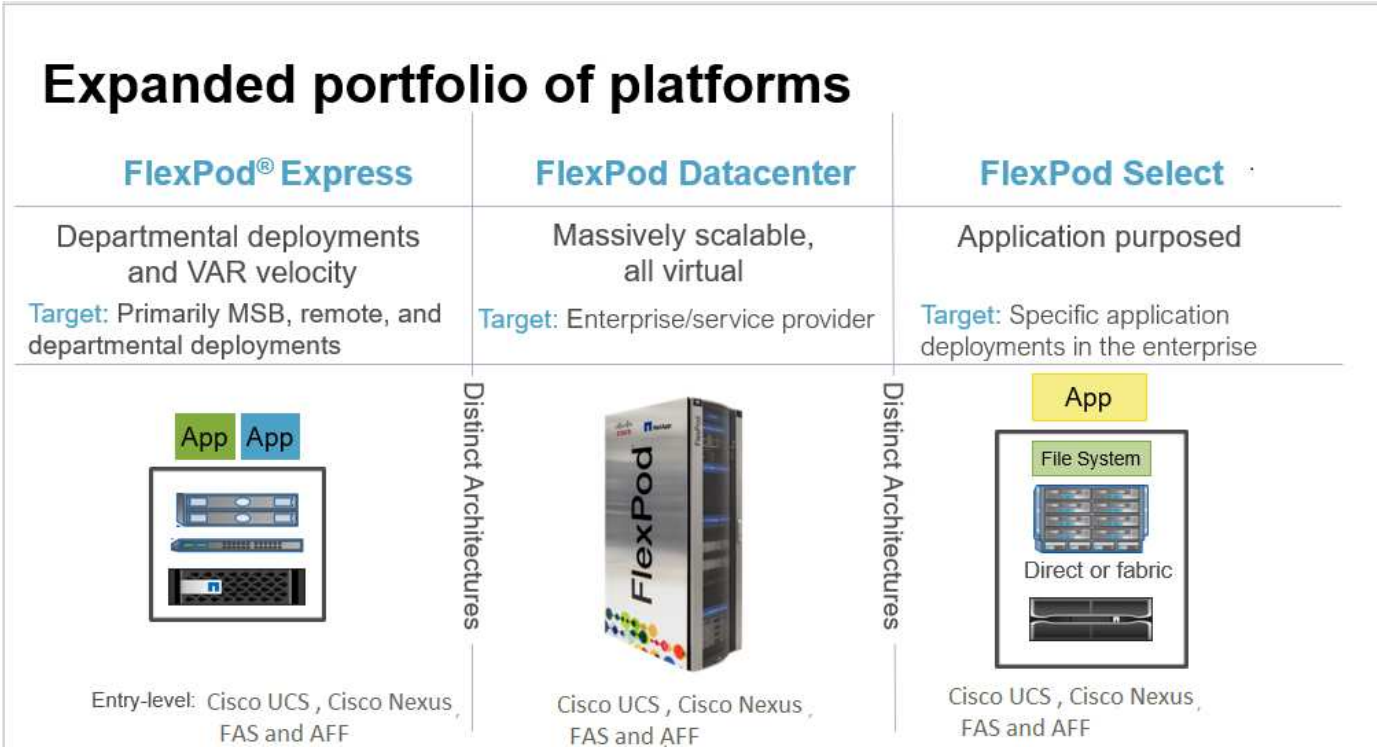
프로그램 요약

FlexPod 통합 인프라 포트폴리오

FlexPod 참조 아키텍처는 CVD(Cisco Validated Design) 또는 NVA(NetApp Verified Architecture)로 제공됩니다. 특정 CVD 또는 NVA의 고객 요구 사항을 기반으로 편차가 지원되지 않는 구성을 구축해야 하는 경우 허용됩니다.

다음 그림과 같이 FlexPod 포트폴리오에는 FlexPod 익스프레스, FlexPod 데이터 센터 및 FlexPod 선택의 세 가지 솔루션이 포함되어 있습니다.

- * FlexPod 익스프레스. * 는 Cisco와 NetApp의 기술로 구성된 엔트리 레벨 솔루션을 제공합니다.
- * FlexPod 데이터 센터 * 는 다양한 워크로드 및 애플리케이션을 위한 최적의 다목적 토대를 제공합니다.
- * FlexPod 선택. * FlexPod 데이터 센터의 최고 기능을 통합하고 특정 애플리케이션에 맞게 인프라를 조정합니다.



NetApp 검증 아키텍처 프로그램

NVA 프로그램은 NetApp 솔루션을 위한 검증된 아키텍처를 고객에게 제공합니다. NVA는 NetApp 솔루션의 다음과 같은 특징을 의미합니다.

- 철저한 테스트를 거친 아키텍처
- 기본적으로 규범적인 아키텍처
- 구축 위험 최소화
- 출시 시기를 단축합니다

이 가이드에서는 VMware vSphere를 사용한 FlexPod Express 설계에 대해 자세히 설명합니다. 또한, 이 설계는 NetApp ONTAP 9.4 소프트웨어, Cisco Nexus 3172P 스위치 및 Cisco UCS C220 M5 서버를 하이퍼바이저 노드로 실행하는 완전히 새로운 AFF A220 시스템을 활용합니다.

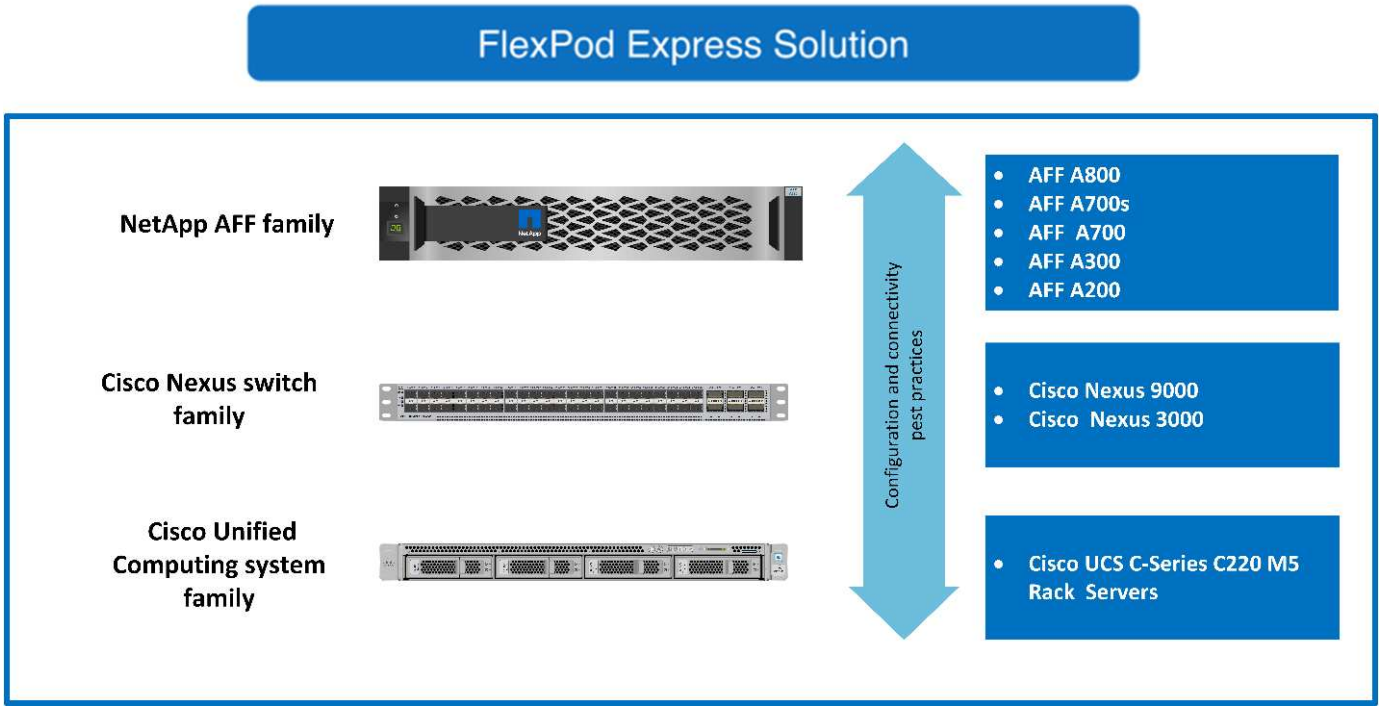
이 문서는 AFF A220에서 검증되었습니다. 하지만 이 솔루션은 FAS2700도 지원합니다.

"다음: 솔루션 개요"

솔루션 개요

FlexPod Express는 혼합 가상화 워크로드를 실행하도록 설계되었습니다. 원격 사무소, 지점 및 중소 및 중견 기업을 타겟으로 합니다. 또한 전용 솔루션을 특정 목적에 구축하고자 하는 대규모 기업에도 적합합니다. FlexPod Express를 위한 이 새로운 솔루션에는 NetApp ONTAP 9.4, NetApp AFF A220 및 VMware vSphere 6.7과 같은 새로운 기술이 추가되었습니다.

다음 그림에서는 FlexPod Express 솔루션에 포함된 하드웨어 구성 요소를 보여 줍니다.

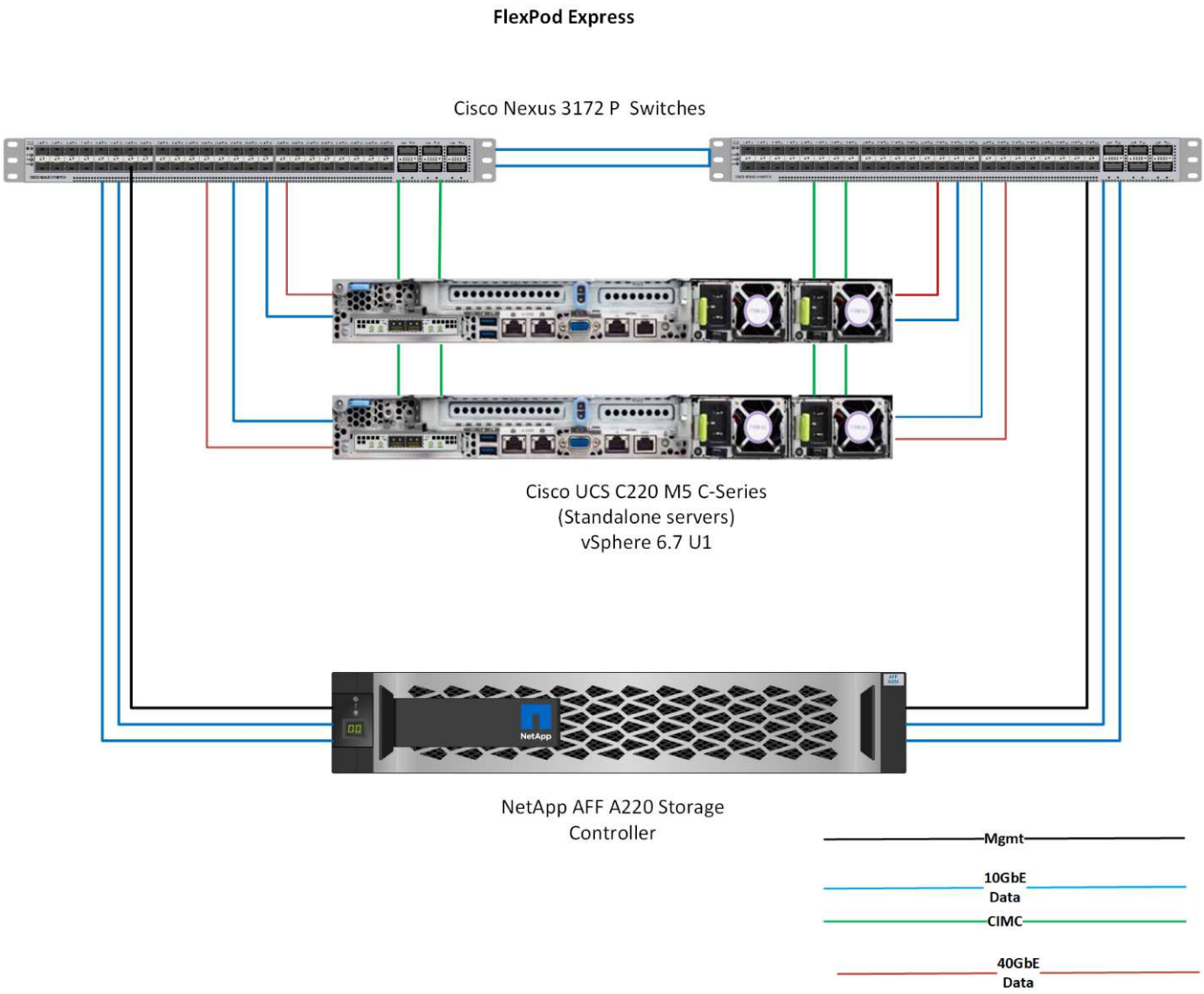


대상

이 문서는 IT 효율성을 제공하고 IT 혁신을 지원하는 인프라를 활용하려는 사용자를 위해 작성되었습니다. 이 문서의 대상에는 세일즈 엔지니어, 현장 컨설턴트, 프로페셔널 서비스 직원, IT 매니저, 파트너 엔지니어 및 고객.

솔루션 기술

이 솔루션은 NetApp, Cisco 및 VMware의 최신 기술을 활용합니다. 이 솔루션에는 ONTAP 9.4 소프트웨어, 이중 Cisco Nexus 3172P 스위치 및 VMware vSphere 6.7을 실행하는 Cisco UCS C220 M5 랙 서버를 실행하는 새로운 NetApp AFF A220 시스템이 포함되어 있습니다. 이 검증된 솔루션은 10기가비트 이더넷(10GbE) 기술을 사용합니다. 다음 그림에서는 개요를 보여 줍니다. 또한 FlexPod 익스프레스 아키텍처가 조직의 변화하는 비즈니스 요구에 적응할 수 있도록 한 번에 두 개의 하이퍼바이저 노드를 추가하여 확장하는 방법에 대한 지침도 제공됩니다.



40GbE는 검증되지 않았지만 지원되는 인프라입니다.

"다음: 기술 요구 사항."

기술 요구 사항

FlexPod Express를 사용하려면 선택한 하이퍼바이저와 네트워크 속도에 따라 하드웨어 및 소프트웨어 구성요소를 조합해야 합니다. 또한 FlexPod Express는 하이퍼바이저 노드를 시스템에 추가하는 데 필요한 하드웨어 구성요소를 2개 단위로 배치합니다.

하드웨어 요구 사항

선택한 하이퍼바이저에 관계없이 모든 FlexPod Express 구성은 동일한 하드웨어를 사용합니다. 따라서 비즈니스 요구사항이 변경되더라도 두 하이퍼바이저 중 하나를 동일한 FlexPod Express 하드웨어에서 실행할 수 있습니다.

다음 표에는 모든 FlexPod Express 구성과 솔루션 구축에 필요한 하드웨어 구성요소가 나와 있습니다. 이 솔루션을 구체적으로 구축하는 데 사용되는 하드웨어 구성요소는 고객 요구사항에 따라 다를 수 있습니다.

하드웨어	수량
AFF A220 2노드 클러스터	1
Cisco UCS C220 M5 서버	2
Cisco Nexus 3172P 스위치	2
Cisco UCS C220 M5 랙 서버용 Cisco UCS VIC(Virtual Interface Card) 1387	2
Cisco CVR-QSFP-SFP 10G 어댑터	4

소프트웨어 요구 사항

다음 표에서는 FlexPod Express 솔루션의 아키텍처를 구현하는 데 필요한 소프트웨어 구성 요소를 보여 줍니다.

다음 표에는 기본 FlexPod Express 구현에 대한 소프트웨어 요구 사항이 나와 있습니다.

소프트웨어	버전	세부 정보
CIMC(Cisco Integrated Management Controller)	3.1.3	C220 M5 랙 서버용
Cisco NX-OS입니다	nxos.7.0.3.I7.5.bin	Cisco Nexus 3172P 스위치용
NetApp ONTAP를 참조하십시오	9.4	AFF A220 컨트롤러

다음 표에는 FlexPod Express의 모든 VMware vSphere 구축에 필요한 소프트웨어가 나와 있습니다.

소프트웨어	버전
VMware vCenter Server 어플라이언스	6.7
VMware vSphere ESXi	6.7
ESXi용 NetApp VAAI 플러그인	1.1.2

"다음: 디자인 선택."

디자인 선택

이 설계를 설계하는 과정에서 다음과 같은 기술이 선택되었습니다. 각 기술은 FlexPod 익스프레스 인프라 솔루션에서 특정 목적에 부합합니다.

NetApp AFF A220 시리즈(ONTAP 9.4 포함)

이 솔루션은 NetApp AFF A220과 ONTAP 9.4 소프트웨어 등 두 가지 최신 NetApp 제품을 활용합니다.

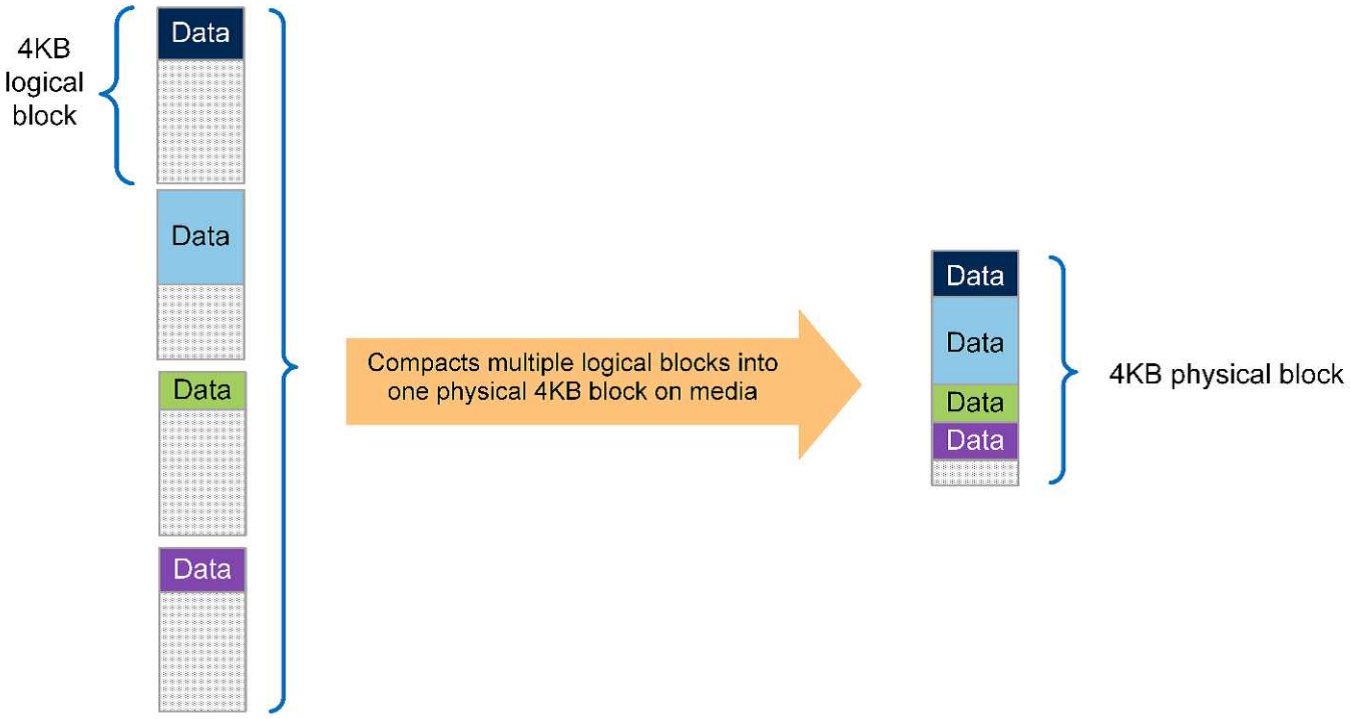
AFF A220 시스템

AFF A220 하드웨어 시스템에 대한 자세한 내용은 를 참조하십시오 "AFF A 시리즈 홈 페이지".

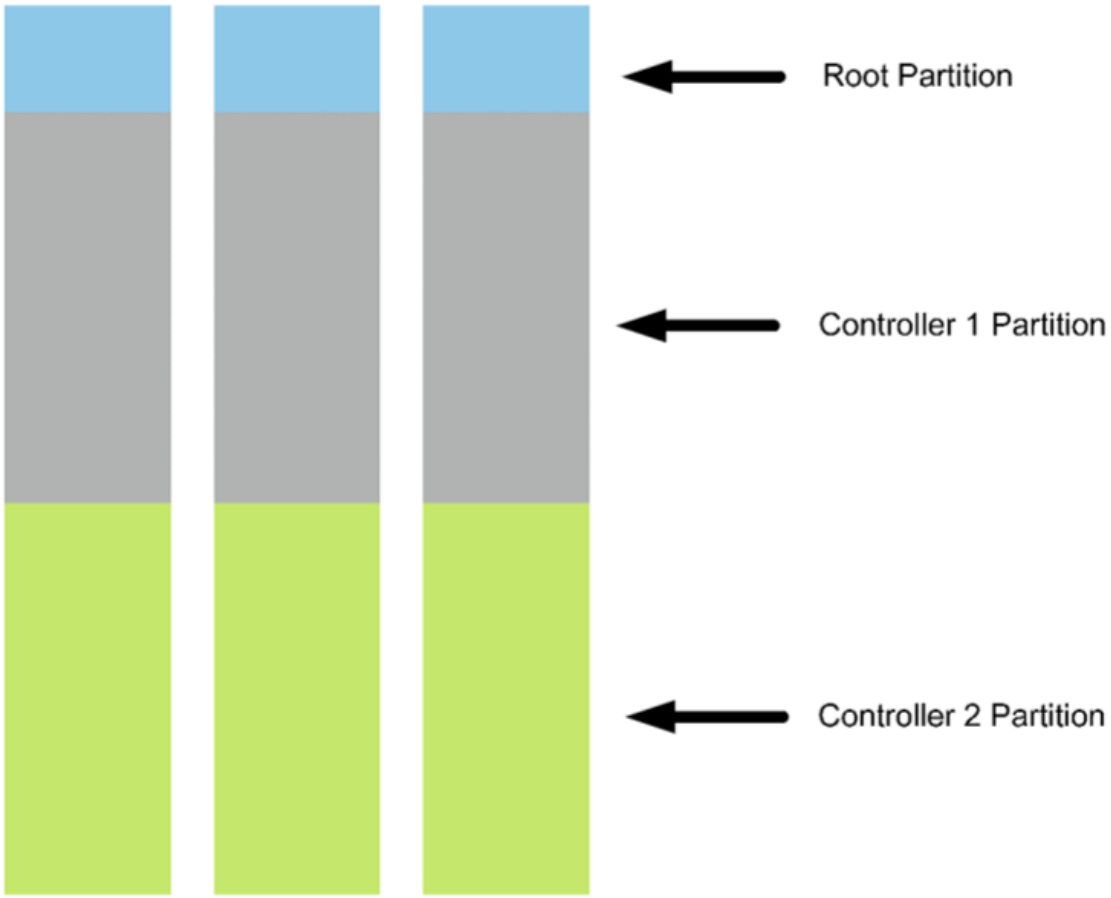
ONTAP 9.4 소프트웨어

NetApp AFF A220 시스템은 새로운 ONTAP 9.4 소프트웨어를 사용합니다. ONTAP 9.4는 업계 최고의 엔터프라이즈 데이터 관리 소프트웨어입니다. 새로운 버전에는 새로운 수준의 단순성과 유연성, 강력한 데이터 관리 기능, 스토리지 효율성, 업계 최고 수준의 클라우드 통합이 결합되어 있습니다.

ONTAP 9.4에는 FlexPod Express 솔루션에 적합한 여러 기능이 있습니다. 가장 중요한 것은 NetApp이 스토리지 효율성을 위해 노력하고 있다는 점입니다. 이는 소규모 구축에 있어서 가장 중요한 기능 중 하나입니다. 중복제거, 압축, 씬 프로비저닝과 같은 NetApp 스토리지 효율성 기능의 특징은 ONTAP 9.4에 새로 추가된 압축 기능입니다. NetApp WAFL 시스템은 항상 4KB 블록을 쓰기 때문에 컴팩션은 블록이 4KB의 할당된 공간을 사용하지 않을 때 여러 블록을 4KB 블록으로 결합합니다. 다음 그림에서는 이 프로세스를 보여 줍니다.



또한 AFF A220 시스템에서 루트 데이터 파티셔닝을 활용할 수 있습니다. 이러한 파티셔닝으로 루트 애그리게이트 및 두 데이터 애그리게이트를 시스템의 디스크에 스트라이핑할 수 있습니다. 따라서 2노드 AFF A220 클러스터의 두 컨트롤러는 aggregate에 있는 모든 디스크의 성능을 활용할 수 있습니다. 다음 그림을 참조하십시오.



이러한 기능은 FlexPod 익스프레스 솔루션을 보완하는 몇 가지 핵심 기능일 뿐입니다. ONTAP 9.4의 추가 기능에 대한 자세한 내용은 를 참조하십시오 "ONTAP 9 데이터 관리 소프트웨어 데이터시트입니다". 또한 "ONTAP 9 문서 센터" ONTAP 9.4를 포함하도록 업데이트된 NetApp를 참조하십시오.

Cisco Nexus 3000 시리즈

Cisco Nexus 3172P는 1/10/40/100Gbps 스위칭을 제공하는 강력하고 비용 효율적인 스위치입니다. Cisco Nexus 3172PQ 스위치는 Unified Fabric 제품군의 일부로서 랙 상단형 데이터 센터 구축을 위한 소형 1랙 유닛(1RU) 스위치입니다. (다음 그림 참조) 1RU에서 최대 72개의 1/10GbE 포트 또는 48개의 1/10GbE 포트를 제공하며 1RU에서 6개의 40GbE 포트를 제공합니다. 또한 물리적 계층의 유연성을 극대화하기 위해 1/10/40Gbps를 지원합니다.

다양한 Cisco Nexus 시리즈 모델이 동일한 기본 운영 체제인 NX-OS를 실행하므로 FlexPod Express 및 FlexPod Datacenter 솔루션에서 여러 Cisco Nexus 모델이 지원됩니다.

성능 사양은 다음과 같습니다.

- 모든 포트에서 회선 속도 트래픽 처리량(계층 2와 3 모두
- 최대 9216바이트(점보 프레임)의 구성 가능한 최대 전송 단위(MTU)

Cisco Nexus 3172 스위치에 대한 자세한 내용은 을 참조하십시오 "Cisco Nexus 3172PQ, 3172TQ, 3172TQ-32T, 3172PQ-XL 및 3172TQ-XL 스위치 데이터 시트".

Cisco UCS C-Series 를 참조하십시오

FlexPod 익스프레스 구축에서는 다양한 구성 옵션으로 Cisco UCS C-Series 랙 서버를 FlexPod 익스프레스 설치시 특정 요구사항에 맞게 구성할 수 있기 때문에 Cisco UCS C-Series 랙 서버를 선택했습니다.

Cisco UCS C-Series 랙 서버는 업계 표준 폼 팩터에서 유니파이드 컴퓨팅을 제공하여 TCO를 절감하고 민첩성을 향상합니다.

Cisco UCS C-Series 랙 서버는 다음과 같은 이점을 제공합니다.

- Cisco UCS의 폼 팩터 중립적인 엔트리 레벨
- 애플리케이션을 간편하고 신속하게 구축
- 통합 컴퓨팅 혁신 및 이점을 랙 서버로 확장
- 친숙한 랙 패키지의 고유한 이점을 통해 고객의 선택 옵션 증가

이전 그림의 Cisco UCS C220 M5 랙 서버(이전 그림 참조)는 업계에서 가장 다양한 범용 엔터프라이즈 인프라 및 애플리케이션 서버 중 하나입니다. 이 서버는 가상화, 협업 및 베어 메탈 애플리케이션을 비롯하여 광범위한 워크로드에 업계 최고의 성능과 효율성을 제공하는 고밀도 2소켓 랙 서버입니다. Cisco UCS C-Series 랙 서버는 독립형 서버로 또는 Cisco UCS의 일부로 구축할 수 있으므로 Cisco의 표준 기반 통합 컴퓨팅 혁신 기술을 활용하여 고객의 TCO를 줄이고 비즈니스 민첩성을 높일 수 있습니다.

C220 M5 서버에 대한 자세한 내용은 를 참조하십시오 "Cisco UCS C220 M5 랙 서버 데이터 시트".

C220 M5 랙 서버용 연결 옵션

C220 M5 랙 서버의 연결 옵션은 다음과 같습니다.

- * Cisco UCS VIC 1387 *

  Cisco UCS VIC 1387(다음 그림 참조)은 모듈식-LAN-On-Motherboard(mLOM) 폼 팩터에서 이중 포트 확장 QSFP+ 40GbE 및 FCoE(FC over Ethernet)를 제공합니다. mLOM 슬롯을 사용하면 PCIe(Peripheral Component Interconnect Express) 슬롯을 사용하지 않고도 Cisco VIC를 설치할 수 있으므로 I/O 확장성이 향상됩니다.

Cisco UCS VIC 1387 어댑터에 대한 자세한 내용은 를 참조하십시오 "Cisco UCS 가상 인터페이스 카드 1387" 데이터 시트.

- * CVR-QSFP-SFP 10G 어댑터 *

  Cisco QSA 모듈은 QSFP 포트를 SFP 또는 SFP+ 포트로 변환합니다. 이 어댑터를 사용하는 고객은 SFP+ 또는 SFP 모듈 또는 케이블을 사용하여 네트워크의 다른 쪽 끝에 있는 저속 포트에 연결할 수 있습니다. 이러한 유연성 덕분에 고밀도 40GbE QSFP 플랫폼의 사용을 극대화하여 40GbE로 비용 효율적으로 전환할 수 있습니다. 이 어댑터는 모든 SFP+ 광학 및 케이블 연결 장치를 지원하며 여러 1GbE SFP 모듈을 지원합니다. 이 프로젝트는 10GbE 연결을 사용하여 검증되었으며 VIC 1387이 40GbE이기 때문에 다음 그림에 나와 있는 CVR-QSFP-SFP SFP 10G 어댑터가 변환에 사용됩니다.

VMware vSphere 6.7을 참조하십시오

VMware vSphere 6.7은 FlexPod Express와 함께 사용할 수 있는 하나의 하이퍼바이저 옵션입니다. VMware vSphere를 사용하면 구입한 컴퓨팅 용량을 최대한 활용하는 동시에 전력 및 냉각 설치 공간을 줄일 수 있습니다. 또한 VMware vSphere를 사용하면 vSphere 호스트 클러스터(VMware Distributed Resource Scheduler 또는 VMware DRS)에서 하드웨어 장애 보호(VMware High Availability 또는 VMware HA)와 컴퓨팅 리소스 로드 밸런싱을 수행할 수 있습니다.

VMware vSphere 6.7은 커널만 다시 시작하므로 고객은 하드웨어를 다시 시작하지 않고 vSphere ESXi를 로드하는 "빠른 부팅"을 수행할 수 있습니다. 이 기능은 빠른 부팅 허용 목록에 있는 플랫폼 및 드라이버에서만 사용할 수

있습니다. vSphere 6.7은 vSphere Web Client의 기능 중 약 90%를 수행할 수 있는 vSphere Client의 기능을 확장합니다.

vSphere 6.7에서 VMware는 고객이 호스트 단위가 아닌 VM(가상 머신)별로 EVC(Enhanced vMotion Compatibility)를 설정할 수 있도록 이 기능을 확장했습니다. vSphere 6.7에서 VMware는 즉각적인 클론을 생성하는 데 사용할 수 있는 API도 공개했습니다.

다음은 vSphere 6.7 U1의 몇 가지 기능입니다.

- HTML5 웹 기반 vSphere Client의 모든 기능을 갖추고 있습니다
- vMotion을 사용하여 NVIDIA GRID vGPU VM을 지원합니다. 인텔 FPGA 지원.
- vCenter Server Converge Tool을 사용하여 외부 PSC에서 내부 PC로 이동합니다.
- vSAN(HCI 업데이트)의 향상된 기능.
- 향상된 콘텐츠 라이브러리.

vSphere 6.7 U1에 대한 자세한 내용은 을 참조하십시오 "vCenter Server 6.7 업데이트 1의 새로운 기능". 이 솔루션은 vSphere 6.7에서 검증되었지만 NetApp Interoperability Matrix Tool에 의해 다른 구성 요소와 함께 검증된 모든 vSphere 버전을 지원합니다. 수정 및 향상된 기능을 위해 vSphere 6.7U1을 구축하는 것이 좋습니다.

부트 아키텍처

다음은 FlexPod 익스프레스 부트 아키텍처에서 지원되는 옵션입니다.

- iSCSI SAN LUN 을 선택합니다
- Cisco FlexFlash SD 카드
- 로컬 디스크

FlexPod 데이터 센터는 iSCSI LUN에서 부팅되므로 FlexPod 익스프레스에 iSCSI 부트를 사용하여 솔루션 관리성이 향상됩니다.

"다음: 솔루션 검증."

솔루션 검증

Cisco와 NetApp은 고객을 위한 최고의 인프라 플랫폼 역할을 할 수 있도록 FlexPod Express를 설계 및 구축했습니다. 업계 최고의 구성 요소로 설계되었기 때문에 고객은 FlexPod Express를 인프라 기반으로 신뢰할 수 있습니다. FlexPod 포트폴리오의 기본 원칙에 따라 FlexPod Express 아키텍처는 Cisco 및 NetApp 데이터 센터 설계자와 엔지니어가 철저히 테스트했습니다. 중복성 및 가용성부터 개별 기능에 이르기까지 전체 FlexPod Express 아키텍처는 고객에 대한 신뢰를 유지하고 설계 프로세스에 대한 신뢰를 구축하는 것으로 검증되었습니다.

VMware vSphere 6.7은 FlexPod Express 인프라스트럭처 구성 요소에서 검증되었습니다. 이 검증에는 하이퍼바이저를 위한 10GbE 업링크 연결 옵션이 포함되었습니다.

"다음: 결론."

결론

FlexPod Express는 업계 최고의 구성요소를 사용하는 검증된 설계를 통해 간단하고 효율적인 솔루션을 제공합니다. FlexPod Express는 하이퍼바이저 플랫폼을 위한 옵션을 제공하고 확장하여 특정 비즈니스 요구에 맞게 조정할 수 있습니다. FlexPod Express는 중소 및 중견 기업, 원격 사무소, 지사 및 전용 솔루션이 필요한 기타 기업을 염두에 두고 설계되었습니다.

"다음: 추가 정보를 찾을 위치."

추가 정보를 찾을 수 있는 위치

이 문서에 설명된 정보에 대한 자세한 내용은 다음 문서 및 웹 사이트를 참조하십시오.

- NetApp 설명서

  "https://docs.netapp.com"

- FlexPod Express with VMware vSphere 6.7 및 NetApp AFF A220 구축 가이드 를 참조하십시오

  "https://www.netapp.com/us/media/nva-1123-deploy.pdf"

FlexPod Express with Cisco UCS C-Series and AFF A220 Series 구축 가이드 를 참조하십시오

NVA-1123-deploy:FlexPod Express with VMware vSphere 6.7 and NetApp AFF A220 구축 가이드

Savita Kumari, NetApp에서 기술 지원

파트너 후원: 

업계 동향에 따르면 많은 데이터 센터가 공유 인프라 및 클라우드 컴퓨팅으로 전환하고 있습니다. 또한 기업에서는 데이터 센터에 친숙한 기술을 활용하여 원격 사무소 및 지사를 위한 간편하고 효율적인 솔루션을 찾고 있습니다.

FlexPod Express는 Cisco UCS(Cisco Unified Computing System), Cisco Nexus 스위치 제품군, NetApp 스토리지 기술을 기반으로 사전 설계되고 모범 사례 데이터 센터 아키텍처입니다. FlexPod 익스프레스 시스템의 구성요소는 FlexPod 데이터 센터와 비슷하기 때문에 더 작은 규모로 전체 IT 인프라 환경에서 관리 시너지 효과를 실현할 수 있습니다. FlexPod 데이터 센터 및 FlexPod 익스프레스는 가상화 및 베어 메탈 운영 체제 및 엔터프라이즈 워크로드를 위한 최적의 플랫폼입니다.

FlexPod 데이터 센터 및 FlexPod 익스프레스는 기본 구성을 제공하며 다양한 사용 사례 및 요구 사항을 수용할 수 있도록 크기를 조정할 수 있는 유연성을 갖추고 있습니다. 기존 FlexPod 데이터 센터 고객은 익숙한 툴을 사용하여 FlexPod 익스프레스 시스템을 관리할 수 있습니다. 새로운 FlexPod Express 고객은 환경 확장에 따라 FlexPod 데이터 센터 관리에 쉽게 적응할 수 있습니다.

FlexPod Express는 원격 사무소, 지점 및 중소기업을 위한 최적의 인프라 기반입니다. 전용 워크로드에 대한 인프라를 제공하려는 고객에게 최적의 솔루션입니다.

FlexPod Express는 거의 모든 워크로드에 적합한 관리하기 쉬운 인프라를 제공합니다.

솔루션 개요

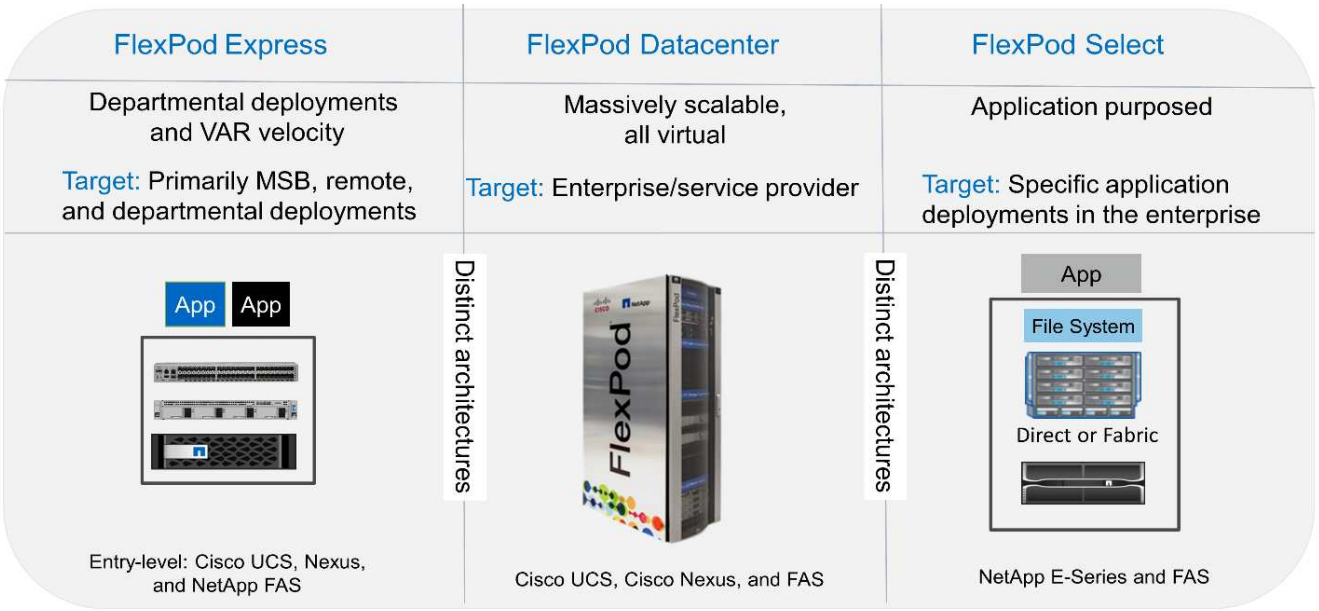
이 FlexPod 익스프레스 솔루션은 FlexPod 통합 인프라 프로그램의 일부입니다.

FlexPod 통합 인프라 프로그램

FlexPod 참조 아키텍처는 CVD(Cisco Validated Design) 또는 NVA(NetApp Verified Architecture)로 제공됩니다. 지정된 CVD 또는 NVA의 고객 요구 사항에 따른 편차는 이러한 변형으로 지원되지 않는 구성이 생성되지는 않을 경우 허용됩니다.

아래 그림과 같이 FlexPod 프로그램에는 FlexPod 익스프레스, FlexPod 데이터 센터, FlexPod 선택의 세 가지 솔루션이 포함되어 있습니다.

- * FlexPod 익스프레스. * 는 Cisco 및 NetApp의 기술을 갖춘 엔트리 레벨 솔루션을 고객에게 제공합니다.
- * FlexPod 데이터 센터 * 는 다양한 워크로드 및 애플리케이션을 위한 최적의 다목적 토대를 제공합니다.
- * FlexPod 선택. * FlexPod 데이터 센터의 최고 기능을 통합하고 특정 애플리케이션에 맞게 인프라를 조정합니다.



NetApp 검증 아키텍처 프로그램

NetApp 검증 아키텍처 프로그램에서는 NetApp 솔루션을 위한 검증된 아키텍처를 고객에게 제공합니다. NetApp 검증 아키텍처는 다음과 같은 품질의 NetApp 솔루션 아키텍처를 제공합니다.

- 철저한 테스트를 거친 아키텍처

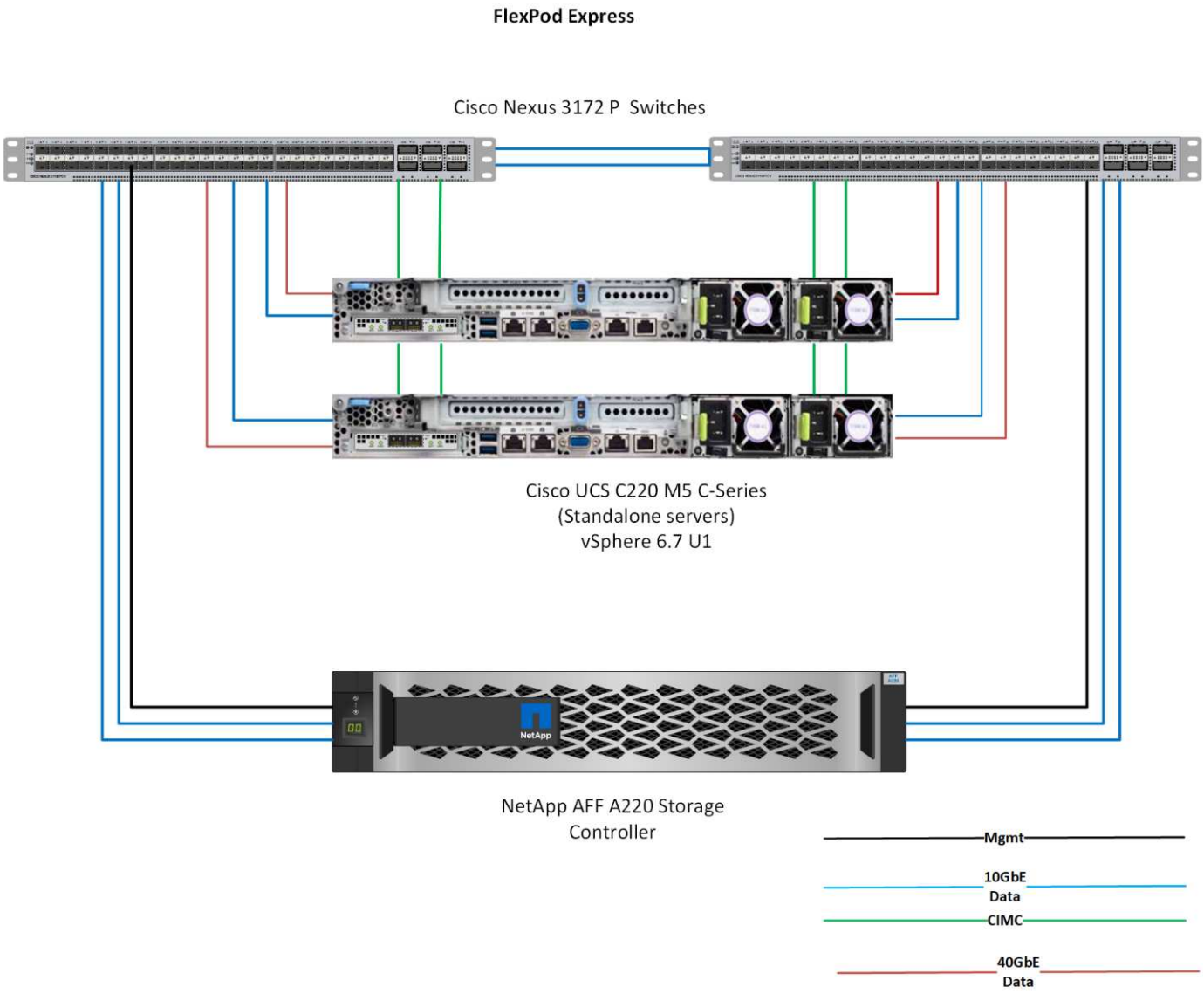
- 기본적으로 규범적인 아키텍처
- 구축 위험 최소화
- 출시 시기를 단축합니다

이 가이드에서는 VMware vSphere를 사용한 FlexPod Express 설계에 대해 자세히 설명합니다. 또한, 이 설계는 NetApp ONTAP 9.4, Cisco Nexus 3172P, Cisco UCS C-Series C220 M5 서버를 하이퍼바이저 노드로 실행하는 완전히 새로운 AFF A220 시스템을 사용합니다.

솔루션 기술

이 솔루션은 NetApp, Cisco 및 VMware의 최신 기술을 활용합니다. 이 솔루션에는 ONTAP 9.4, 이중 Cisco Nexus 3172P 스위치 및 VMware vSphere 6.7을 실행하는 Cisco UCS C220 M5 랙 서버를 실행하는 새로운 NetApp AFF A220이 포함되어 있습니다. 이 검증된 솔루션은 10GbE 기술을 사용합니다. 또한 FlexPod 익스프레스 아키텍처가 조직의 변화하는 비즈니스 요구에 적응할 수 있도록 한 번에 두 개의 하이퍼바이저 노드를 추가하여 컴퓨팅 용량을 확장하는 방법에 대한 지침도 제공됩니다.

다음 그림에서는 VMware vSphere 10GbE 아키텍처를 사용하는 FlexPod Express를 보여 줍니다.



이 검증에서는 10GbE 연결과 40GbE의 Cisco UCS VIC 1387을 사용합니다. 10GbE 연결을 위해 CVR-QSFP-SFP-SFP 10G 어댑터가 사용됩니다.

사용 사례 요약

FlexPod 익스프레스 솔루션은 다음과 같은 여러 사용 사례에 적용할 수 있습니다.

- 원격 사무소 및 지사
- 중소기업
- 비용 효율적인 전용 솔루션이 필요한 환경

FlexPod Express는 가상화된 혼합 워크로드에 가장 적합합니다.

이 솔루션은 vSphere 6.7에서 검증되었지만 NetApp Interoperability Matrix Tool에 의해 다른 구성 요소와 함께 검증된 모든 vSphere 버전을 지원합니다. 수정 및 향상된 기능을 위해 vSphere 6.7U1을 구축하는 것이 좋습니다.

다음은 vSphere 6.7 U1의 몇 가지 기능입니다.

- HTML5 웹 기반 vSphere Client의 모든 기능을 갖추고 있습니다
- vMotion을 사용하여 NVIDIA GRID vGPU VM을 지원합니다. 인텔 FPGA 지원
- vCenter Server Converge Tool을 사용하여 외부 PSC에서 내부 PC로 이동합니다
- vSAN(HCI 업데이트) 기능 향상
- 향상된 콘텐츠 라이브러리

vSphere 6.7 U1에 대한 자세한 내용은 을 참조하십시오 "vCenter Server 6.7 업데이트 1의 새로운 기능".

기술 요구 사항

FlexPod 익스프레스 시스템에는 하드웨어 및 소프트웨어 구성 요소의 조합이 필요합니다. 또한 FlexPod Express는 하이퍼바이저 노드를 시스템에 추가하는 데 필요한 하드웨어 구성요소를 2개 단위로 설명합니다.

하드웨어 요구 사항

선택한 하이퍼바이저에 관계없이 모든 FlexPod Express 구성은 동일한 하드웨어를 사용합니다. 따라서 비즈니스 요구사항이 변경되더라도 두 하이퍼바이저 중 하나를 동일한 FlexPod Express 하드웨어에서 실행할 수 있습니다.

다음 표에는 모든 FlexPod Express 구성에 필요한 하드웨어 구성요소가 나와 있습니다.

하드웨어	수량
AFF A220 HA 쌍	1
Cisco C220 M5 서버	2
Cisco Nexus 3172P 스위치	2

하드웨어	수량
C220 M5 서버용 Cisco UCS 가상 인터페이스 카드(VIC) 1387	2
CVR-QSFP-SFP 10G 어댑터	4

다음 표에는 10GbE 구현을 위한 기본 구성 외에 필요한 하드웨어가 나와 있습니다.

하드웨어	수량
Cisco UCS C220 M5 서버	2
Cisco VIC 1387	2
CVR-QSFP-SFP 10G 어댑터	4

소프트웨어 요구 사항

다음 표에는 FlexPod Express 솔루션의 아키텍처를 구현하는 데 필요한 소프트웨어 구성 요소가 나열되어 있습니다.

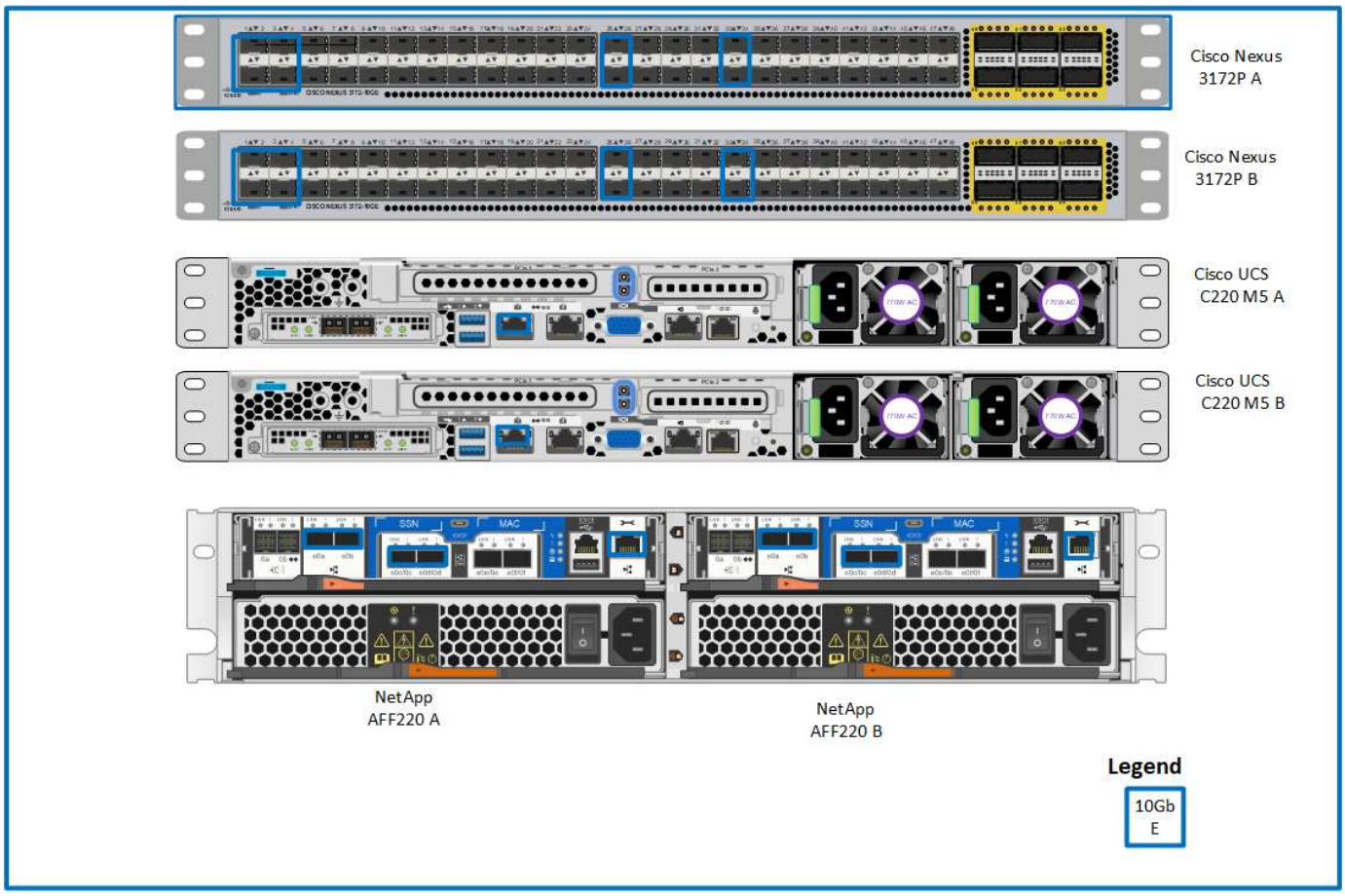
소프트웨어	버전	세부 정보
CIMC(Cisco Integrated Management Controller)	3.1(3G)	Cisco UCS C220 M5 랙 서버용
Cisco nenic 드라이버	1.0.25.0	VIC 1387 인터페이스 카드의 경우
Cisco NX-OS입니다	nxos.7.0.3.I7.5.bin	Cisco Nexus 3172P 스위치용
NetApp ONTAP를 참조하십시오	9.4	AFF A220 컨트롤러

다음 표에는 FlexPod Express의 모든 VMware vSphere 구축에 필요한 소프트웨어가 나와 있습니다.

소프트웨어	버전
VMware vCenter Server 어플라이언스	6.7
VMware vSphere ESXi 하이퍼바이저	6.7
ESXi용 NetApp VAAI 플러그인	1.1.2

FlexPod Express 케이블링 정보

다음 그림은 참조 검증 케이블 연결을 보여 줍니다.



다음 표에서는 Cisco Nexus 스위치 3172P A 의 케이블 연결 정보를 보여 줍니다

로컬 장치	로컬 포트	원격 장치	원격 포트
Cisco Nexus 스위치 3172P A	eth1/1	NetApp AFF A220 스토리지 컨트롤러 A입니다	e0c
	eth1/2	NetApp AFF A220 스토리지 컨트롤러 B입니다	e0c
	eth1/3	Cisco UCS C220 C-Series 독립 실행형 서버 A	CVR-QSFP-SFP 10G 어댑터가 있는 MLOM1
	eth1/4	Cisco UCS C220 C-Series 독립 실행형 서버 B	CVR-QSFP-SFP 10G 어댑터가 있는 MLOM1
	eth1/25	Cisco Nexus 스위치 3172P B	eth1/25
	Eth1/26	Cisco Nexus 스위치 3172P B	Eth1/26
	Eth1/33	NetApp AFF A220 스토리지 컨트롤러 A입니다	e0M
	eth1/34	Cisco UCS C220 C-Series 독립 실행형 서버 A	CIMC를 참조하십시오

다음 표에서는 Cisco Nexus 스위치 3172P B 의 케이블 연결 정보를 보여 줍니다

로컬 장치	로컬 포트	원격 장치	원격 포트
Cisco Nexus 스위치 3172P B	eth1/1	NetApp AFF A220 스토리지 컨트롤러 A입니다	e0d
	eth1/2	NetApp AFF A220 스토리지 컨트롤러 B입니다	e0d
	eth1/3	Cisco UCS C220 C-Series 독립 실행형 서버 A	CVR-QSFP-SFP 10G 어댑터가 포함된 MLOM2
	eth1/4	Cisco UCS C220 C-Series 독립 실행형 서버 B	CVR-QSFP-SFP 10G 어댑터가 포함된 MLOM2
	eth1/25	Cisco Nexus 스위치 3172P A	eth1/25
	Eth1/26	Cisco Nexus 스위치 3172P A	Eth1/26
	Eth1/33	NetApp AFF A220 스토리지 컨트롤러 B입니다	e0M
	eth1/34	Cisco UCS C220 C-Series 독립 실행형 서버 B	CIMC를 참조하십시오

다음 표에서는 NetApp AFF A220 스토리지 컨트롤러 A의 케이블 연결 정보를 보여 줍니다

로컬 장치	로컬 포트	원격 장치	원격 포트
NetApp AFF A220 스토리지 컨트롤러 A입니다	e0a	NetApp AFF A220 스토리지 컨트롤러 B입니다	e0a
	e0b	NetApp AFF A220 스토리지 컨트롤러 B입니다	e0b
	e0c	Cisco Nexus 스위치 3172P A	eth1/1
	e0d	Cisco Nexus 스위치 3172P B	eth1/1
	e0M	Cisco Nexus 스위치 3172P A	Eth1/33

다음 표에서는 NetApp AFF A220 스토리지 컨트롤러 B의 케이블 연결 정보를 보여 줍니다

로컬 장치	로컬 포트	원격 장치	원격 포트
NetApp AFF A220 스토리지 컨트롤러 B입니다	e0a	NetApp AFF A220 스토리지 컨트롤러 A입니다	e0a
	e0b	NetApp AFF A220 스토리지 컨트롤러 A입니다	e0b
	e0c	Cisco Nexus 스위치 3172P A	eth1/2
	e0d	Cisco Nexus 스위치 3172P B	eth1/2

로컬 장치	로컬 포트	원격 장치	원격 포트
	e0M	Cisco Nexus 스위치 3172P B	Eth1/33

구현 절차

이 문서에서는 완전히 이중화된 고가용성 FlexPod Express 시스템을 구성하는 방법에 대해 자세히 설명합니다. 이러한 이중화를 반영하기 위해 각 단계에서 구성 요소를 구성 요소 A 또는 구성 요소 B라고 합니다 예를 들어 컨트롤러 A와 컨트롤러 B는 이 문서에 프로비저닝된 NetApp 스토리지 컨트롤러 2개를 식별합니다. 스위치 A와 스위치 B는 Cisco Nexus 스위치 쌍을 나타냅니다.

또한 서버 A, 서버 B 등으로 순차적으로 구분되는 여러 Cisco UCS 호스트를 프로비저닝하는 단계도 설명합니다.

사용자 환경과 관련된 정보를 단계별로 포함해야 함을 나타내기 위해 명령 구조의 일부로 '<<text>>'이 표시됩니다. 'VLAN create' 명령은 다음 예를 참조하십시오.

```
Controller01>vlan create vif0 <<mgmt_vlan_id>>
```

이 문서를 사용하여 FlexPod Express 환경을 완전히 구성할 수 있습니다. 이 프로세스에서 다양한 단계를 수행하려면 고객별 명명 규칙, IP 주소 및 VLAN(Virtual Local Area Network) 스키마를 삽입해야 합니다. 아래 표에는 이 가이드에 설명된 대로 구축에 필요한 VLAN이 설명되어 있습니다. 이 표는 특정 사이트 변수를 기반으로 완료할 수 있으며 문서 구성 단계를 구현하는 데 사용할 수 있습니다.

별도의 대역내 및 대역외 관리 VLAN을 사용하는 경우 이러한 VLAN 간에 레이어 3 경로를 만들어야 합니다. 이 검증에서는 공통 관리 VLAN이 사용되었습니다.

이름	**VLAN**의 용도	이 문서의 유효성을 검사하는 데 사용되는 **ID**입니다
관리 VLAN	관리 인터페이스용 VLAN	3437
네이티브 VLAN	태그가 지정되지 않은 프레임이 할당되는 VLAN입니다	2
NFS VLAN	NFS 트래픽용 VLAN	3438
VMware vMotion VLAN	하나의 물리적 호스트에서 다른 물리적 호스트로 가상 시스템을 이동할 수 있도록 지정된 VLAN입니다	3441
가상 머신 트래픽 VLAN	가상 머신 애플리케이션 트래픽용 VLAN	3442
iSCSI-A-VLAN	패브릭 A의 iSCSI 트래픽용 VLAN	3439
iSCSI-B-VLAN	패브릭 B의 iSCSI 트래픽용 VLAN	3440

FlexPod Express를 구성하는 동안 VLAN 번호가 필요합니다. VLAN은 "<<var_xxxx_vlan>>"라고 하며, 여기서 "xxxx"는 VLAN의 목적(예: iSCSI-A)입니다.

아래 표에는 생성된 VMware 가상 머신이 나와 있습니다.

가상 머신 설명입니다	호스트 이름입니다
VMware vCenter Server를 참조하십시오	

Cisco Nexus 3172P 구축 절차

다음 섹션에서는 FlexPod 익스프레스 환경에 사용되는 Cisco Nexus 3172P 스위치 구성에 대해 자세히 설명합니다.

Cisco Nexus 3172P 스위치의 초기 설정

다음 절차에서는 기본 FlexPod Express 환경에서 사용할 Cisco Nexus 스위치를 구성하는 방법에 대해 설명합니다.

> 이 절차에서는 NX-OS 소프트웨어 릴리즈 7.0(3) i7(5)을 실행하는 Cisco Nexus 3172P를 사용하고 있다고 가정합니다.

1. 초기 부팅이 완료되고 스위치의 콘솔 포트에 연결되면 Cisco NX-OS 설정이 자동으로 시작됩니다. 이 초기 구성에서는 스위치 이름, mgmt0 인터페이스 구성, SSH(Secure Shell) 설정과 같은 기본 설정을 지정합니다.
2. FlexPod 익스프레스 관리 네트워크는 여러 가지 방법으로 구성할 수 있습니다. 3172P 스위치의 mgmt0 인터페이스를 기존 관리 네트워크에 연결할 수도 있고, 3172P 스위치의 mgmt0 인터페이스를 연속 연결 구성으로 연결할 수도 있습니다. 하지만 이 링크는 SSH 트래픽과 같은 외부 관리 액세스에 사용할 수 없습니다.

   이 구축 가이드에서는 FlexPod 익스프레스 Cisco Nexus 3172P 스위치를 기존 관리 네트워크에 연결합니다.
3. Cisco Nexus 3172P 스위치를 구성하려면 스위치의 전원을 켠 후 여기 에 나온 것처럼 화면 메시지에 따라 두 스위치를 초기 설정하고 스위치 관련 정보에 적절한 값을 대체하십시오.

```
This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.
*Note: setup is mainly used for configuring the system initially,
when no configuration is present. So setup always assumes system
defaults and not the current system configuration values.
Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.
Would you like to enter the basic configuration dialog (yes/no): y
Do you want to enforce secure password standard (yes/no) [y]: y
  Create another login account (yes/no) [n]: n
  Configure read-only SNMP community string (yes/no) [n]: n
  Configure read-write SNMP community string (yes/no) [n]: n
  Enter the switch name : 3172P-B
  Continue with Out-of-band (mgmt0) management configuration? (yes/no)
[y]: y
    Mgmt0 IPv4 address : <<var_switch_mgmt_ip>>
    Mgmt0 IPv4 netmask : <<var_switch_mgmt_netmask>>
  Configure the default gateway? (yes/no) [y]: y
    IPv4 address of the default gateway : <<var_switch_mgmt_gateway>>
  Configure advanced IP options? (yes/no) [n]: n
  Enable the telnet service? (yes/no) [n]: n
  Enable the ssh service? (yes/no) [y]: y
    Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa
    Number of rsa key bits <1024-2048> [1024]:  <enter>
  Configure the ntp server? (yes/no) [n]: y
    NTP server IPv4 address : <<var_ntp_ip>>
  Configure default interface layer (L3/L2) [L2]: <enter>
  Configure default switchport interface state (shut/noshut) [noshut]:
<enter>
  Configure CoPP system profile (strict/moderate/lenient/dense)
[strict]:  <enter>
```

4. 그러면 구성 요약이 표시됩니다. 구성을 편집할지 묻는 메시지가 나타납니다. 구성이 올바르면 n을 입력합니다.

```
Would you like to edit the configuration? (yes/no) [n]: n
```

5. 그런 다음 이 구성을 사용하고 저장할지 묻는 메시지가 표시됩니다. 그렇다면 y를 입력합니다.

```
Use this configuration and save it? (yes/no) [y]: Enter
```

6. Cisco Nexus 스위치 B에 대해 이 절차를 반복합니다

고급 기능을 활성화합니다

추가 구성 옵션을 제공하려면 Cisco NX-OS에서 특정 고급 기능을 사용하도록 설정해야 합니다.

> interface-vlan 기능은 본 문서 전반에 걸쳐 설명한 back-to-back mgmt0 옵션을 사용하는 경우에만 필요합니다. 이 기능을 사용하면 IP 주소를 인터페이스 VLAN(스위치 가상 인터페이스)에 할당하여 SSH를 통해 스위치에 대한 대역 내 관리 통신을 사용할 수 있습니다.

1. Cisco Nexus 스위치 A와 스위치 B에서 적절한 기능을 활성화하려면 '(config t)' 명령을 사용하여 구성 모드를 시작하고 다음 명령을 실행하십시오.

```
feature interface-vlan
feature lacp
feature vpc
```

   기본 포트 채널 로드 밸런싱 해쉬는 소스 및 타깃 IP 주소를 사용하여 포트 채널의 인터페이스에 대한 로드 밸런싱 알고리즘을 결정합니다. 소스 및 타깃 IP 주소보다 많은 입력을 해쉬 알고리즘에 제공하면 포트 채널 멤버 전체에 걸쳐 더 효율적으로 분산될 수 있습니다. 동일한 이유로 소스 및 타깃 TCP 포트를 해쉬 알고리즘에 추가하는 것이 좋습니다.

2. 구성 모드('config t')에서 다음 명령을 입력하여 Cisco Nexus 스위치 A 및 스위치 B의 글로벌 포트 채널 로드 밸런싱 구성을 설정하십시오.

```
port-channel load-balance src-dst ip-l4port
```

글로벌 스패닝 트리 구성을 수행합니다

Cisco Nexus 플랫폼은 브리지 보장이라는 새로운 보호 기능을 사용합니다. 브리지 보장은 스패닝 트리 알고리즘을 더 이상 실행하지 않는 장치에서 데이터 트래픽을 계속 전달하는 단방향 링크 또는 기타 소프트웨어 장애를 방지합니다. 플랫폼에 따라 네트워크 또는 가장자리를 포함한 여러 상태 중 하나에 포트를 배치할 수 있습니다.

기본적으로 모든 포트가 네트워크 포트로 간주되도록 브리지 보장을 설정하는 것이 좋습니다. 이 설정은 네트워크 관리자가 각 포트의 구성을 검토하도록 합니다. 또한 확인되지 않은 에지 포트 또는 브리지 보장 기능이 활성화되지 않은 인접 장치와 같은 가장 일반적인 구성 오류도 표시됩니다. 또한 스패닝 트리에서 너무 적은 포트가 아니라 많은 포트를 차단하는 편이 더 안전합니다. 그러면 기본 포트 상태를 통해 네트워크의 전반적인 안정성을 향상할 수 있습니다.

특히 브리지 보장을 지원하지 않는 서버, 스토리지 및 업링크 스위치를 추가할 때는 스패닝 트리 상태에 세심한 주의를 기울여야 합니다. 이러한 경우 포트를 활성화하려면 포트 유형을 변경해야 할 수 있습니다.

브리지 프로토콜 데이터 단위(BPDU) 보호대는 기본적으로 다른 보호 계층으로 에지 포트에서 활성화됩니다. 네트워크의 루프를 방지하기 위해 이 기능은 다른 스위치의 BPDU가 이 인터페이스에 표시되는 경우 포트를 종료합니다.

구성 모드('config t')에서 다음 명령을 실행하여 Cisco Nexus 스위치 A 및 스위치 B에서 기본 포트 유형과 BPDU 가드를 포함한 기본 스패닝 트리 옵션을 구성하십시오.

```
spanning-tree port type network default
spanning-tree port type edge bpduguard default
```

VLAN을 정의합니다

VLAN이 서로 다른 개별 포트를 구성하기 전에 스위치에서 계층 2 VLAN을 정의해야 합니다. 향후 문제 해결이 용이하도록 VLAN 이름을 지정하는 것도 좋은 방법입니다.

구성 모드('config t')에서 다음 명령을 실행하여 Cisco Nexus 스위치 A 및 스위치 B의 계층 2 VLAN을 정의하고 설명하십시오.

```
vlan <<nfs_vlan_id>>
  name NFS-VLAN
vlan <<iSCSI_A_vlan_id>>
  name iSCSI-A-VLAN
vlan <<iSCSI_B_vlan_id>>
  name iSCSI-B-VLAN
vlan <<vmotion_vlan_id>>
  name vMotion-VLAN
vlan <<vmtraffic_vlan_id>>
  name VM-Traffic-VLAN
vlan <<mgmt_vlan_id>>
  name MGMT-VLAN
vlan <<native_vlan_id>>
  name NATIVE-VLAN
exit
```

액세스 및 관리 포트 설명을 구성합니다

계층 2 VLAN에 이름을 할당하는 경우와 마찬가지로, 모든 인터페이스에 대한 설정 설명은 프로비저닝과 문제 해결에 도움이 될 수 있습니다.

각 스위치의 구성 모드('config t')에서 FlexPod Express 대규모 구성에 대한 다음 포트 설명을 입력합니다.

Cisco Nexus 스위치 **A**

```
int eth1/1
  description AFF A220-A e0c
int eth1/2
  description AFF A220-B e0c
int eth1/3
  description UCS-Server-A: MLOM port 0
int eth1/4
  description UCS-Server-B: MLOM port 0
int eth1/25
  description vPC peer-link 3172P-B 1/25
int eth1/26
  description vPC peer-link 3172P-B 1/26
int eth1/33
  description AFF A220-A e0M
int eth1/34
  description UCS Server A: CIMC
```

Cisco Nexus 스위치 **B**

```
int eth1/1
  description AFF A220-A e0d
int eth1/2
  description AFF A220-B e0d
int eth1/3
  description UCS-Server-A: MLOM port 1
int eth1/4
  description UCS-Server-B: MLOM port 1
int eth1/25
  description vPC peer-link 3172P-A 1/25
int eth1/26
  description vPC peer-link 3172P-A 1/26
int eth1/33
  description AFF A220-B e0M
int eth1/34
  description UCS Server B: CIMC
```

서버 및 스토리지 관리 인터페이스를 구성합니다

서버와 스토리지 모두의 관리 인터페이스는 일반적으로 단일 VLAN만 사용합니다. 따라서 관리 인터페이스 포트를 액세스 포트로 구성합니다. 각 스위치에 대한 관리 VLAN을 정의하고 스패닝 트리 포트 유형을 에지로 변경합니다.

구성 모드('config t')에서 다음 명령을 입력하여 서버와 스토리지 모두의 관리 인터페이스에 대한 포트 설정을 구성하십시오.

Cisco Nexus 스위치 **A**

```
int eth1/33-34
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

Cisco Nexus 스위치 **B**

```
int eth1/33-34
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

가상 포트 채널 글로벌 구성을 수행합니다

가상 포트 채널(vPC)을 사용하면 물리적으로 두 개의 서로 다른 Cisco Nexus 스위치에 연결된 링크가 세 번째 장치에 단일 포트 채널로 표시될 수 있습니다. 세 번째 장치는 스위치, 서버 또는 다른 네트워킹 장치일 수 있습니다. vPC는 계층 2 다중 경로를 제공할 수 있으므로 대역폭을 높이고, 노드 간에 여러 개의 병렬 경로를 활성화하고, 대체 경로가 있는 로드 밸런싱 트래픽을 통해 이중화를 생성할 수 있습니다.

vPC는 다음과 같은 이점을 제공합니다.

- 단일 장치에서 두 업스트림 장치에 걸쳐 포트 채널을 사용하도록 설정
- 스패닝 트리 프로토콜 차단 포트 제거
- 루프 없는 토폴로지 제공
- 사용 가능한 모든 업링크 대역폭 사용
- 링크 또는 디바이스에 장애가 발생할 경우 빠른 컨버전스를 제공합니다
- 링크 레벨의 복원력 제공
- 고가용성 제공 지원

vPC 기능이 제대로 작동하려면 두 Cisco Nexus 스위치 간의 몇 가지 초기 설정이 필요합니다. 연속 인접 mgmt0 구성을 사용하는 경우에는 인터페이스에 정의된 주소를 사용하고 ping을 사용하여 통신 가능 여부를 확인해야 합니다[switch_A/B_mgmt0_ip_addr]VRF 관리 명령어

구성 모드('config t')에서 다음 명령을 실행하여 두 스위치에 대한 vPC 글로벌 구성을 설정하십시오.

Cisco Nexus 스위치 **A**

```
vpc domain 1
 role priority 10
  peer-keepalive destination <<switch_B_mgmt0_ip_addr>> source
<<switch_A_mgmt0_ip_addr>> vrf management
  peer-gateway
  auto-recovery
  ip arp synchronize
int eth1/25-26
  channel-group 10 mode active
int Po10
  description vPC peer-link
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type network
  vpc peer-link
  no shut
exit
copy run start
```

Cisco Nexus 스위치 B

```
vpc domain 1
  peer-switch
  role priority 20
  peer-keepalive destination <<switch_A_mgmt0_ip_addr>> source
<<switch_B_mgmt0_ip_addr>> vrf management
  peer-gateway
  auto-recovery
  ip arp synchronize
int eth1/25- 26
  channel-group 10 mode active
int Po10
  description vPC peer-link
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type network
  vpc peer-link
no shut
exit
copy run start
```

스토리지 포트 채널을 구성합니다

NetApp 스토리지 컨트롤러는 LACP(Link Aggregation Control Protocol)를 사용하여 네트워크에 대해 active-active 연결을 허용합니다. LACP 사용이 선호되는 이유는 LACP가 스위치 간에 협상과 로깅을 모두 추가하기 때문입니다. 네트워크가 vPC에 맞게 설정되므로 이 접근 방식을 통해 스토리지에서 별도의 물리적 스위치로의 active-active 연결을 설정할 수 있습니다. 각 컨트롤러에는 각 스위치에 대한 링크가 2개 있습니다. 그러나 4개의 링크 모두 동일한 vPC 및 인터페이스 그룹(IFGRP)에 속합니다.

구성 모드('config t')에서 각 스위치에 대해 다음 명령을 실행하여 개별 인터페이스를 구성하고 NetApp AFF 컨트롤러에 연결된 포트에 대한 결과 포트 채널 구성을 설정하십시오.

1. 스위치 A와 스위치 B에서 다음 명령을 실행하여 스토리지 컨트롤러 A의 포트 채널을 구성합니다.

```
int eth1/1
  channel-group 11 mode active
int Po11
  description vPC to Controller-A
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<nfs_vlan_id>>,<<mgmt_vlan_id>>,<<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  vpc 11
  no shut
```

2. 스위치 A와 스위치 B에서 다음 명령을 실행하여 스토리지 컨트롤러 B의 포트 채널을 구성합니다

```
int eth1/2
  channel-group 12 mode active
int Po12
  description vPC to Controller-B
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<mgmt_vlan_id>>,
<<iSCSI_A_vlan_id>>, <<iSCSI_B_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  vpc 12
  no shut
exit
copy run start
```

이 솔루션 검증에서 MTU 9000이 사용되었습니다. 그러나 애플리케이션 요구 사항에 따라 MTU의 적절한 값을 구성할 수 있습니다. FlexPod 솔루션에서 동일한 MTU 값을 설정하는 것이 중요합니다. 구성 요소 간의 MTU 구성이 잘못되면 패킷이 손실되고 이러한 패킷이 생성됩니다.

서버 연결을 구성합니다

Cisco UCS 서버에는 데이터 트래픽과 iSCSI를 사용한 ESXi 운영 체제 부팅에 사용되는 2포트 가상 인터페이스 카드 VIC1387이 있습니다. 이러한 인터페이스는 서로 간에 페일오버되도록 구성되어 단일 링크를 넘어 추가적인 이중화를 제공합니다. 이러한 링크를 여러 스위치에 걸쳐 분산하면 완전한 스위치 장애가 발생해도 서버가 가동 상태를 유지할 수 있습니다.

구성 모드('config t')에서 다음 명령을 실행하여 각 서버에 연결된 인터페이스에 대한 포트 설정을 구성합니다.

Cisco Nexus 스위치 **A: Cisco UCS** 서버 **A** 및 **Cisco UCS** 서버 **B** 구성

```
int eth1/3-4
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<iSCSI_A_vlan_id>>,<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_i
d>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu9216
  no shut
exit
copy run start
```

Cisco Nexus 스위치 **B: Cisco UCS** 서버 **A** 및 **Cisco UCS** 서버 **B** 구성

```
int eth1/3-4
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<iSCSI_B_vlan_id>>,<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_i
d>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  no shut
exit
copy run start
```

이 솔루션 검증에서 MTU 9000이 사용되었습니다. 그러나 애플리케이션 요구 사항에 따라 MTU의 적절한 값을 구성할 수 있습니다. FlexPod 솔루션에서 동일한 MTU 값을 설정하는 것이 중요합니다. 구성 요소 간의 MTU 구성이 잘못되면 패킷이 손실되고 이러한 패킷은 다시 전송되어야 합니다. 이 문제는 솔루션의 전반적인 성능에 영향을 줍니다.

Cisco UCS 서버를 추가하여 솔루션을 확장하거나, 스위치 A 및 B에서 새로 추가한 서버가 연결된 스위치 포트를 사용하여 이전 명령을 실행합니다

기존 네트워크 인프라로 업링크

사용 가능한 네트워크 인프라에 따라 여러 가지 방법과 기능을 사용하여 FlexPod 환경을 업링크할 수 있습니다. 기존 Cisco Nexus 환경이 존재하는 경우, NetApp은 vPC를 사용하여 FlexPod 환경에 포함된 Cisco Nexus 3172P 스위치를 인프라로 업링크하는 것을 권장합니다. 업링크는 10GbE 인프라스트럭처 솔루션의 경우 10GbE 업링크 또는 필요한 경우 1GbE 인프라스트럭처 솔루션의 경우 1GbE일 수 있습니다. 앞서 설명한 절차를 사용하여 기존 환경에 대한 업링크 vPC를 생성할 수 있습니다. 구성이 완료된 후 각 스위치에 대한 구성을 저장하려면 copy run start를 실행해야 합니다.

"다음: NetApp 스토리지 구현 절차(1부)"

NetApp 스토리지 구축 절차(1부)

이 섹션에서는 NetApp AFF 스토리지 구축 절차를 설명합니다.

NetApp 스토리지 컨트롤러 AFF2xx 시리즈 설치

NetApp Hardware Universe를 참조하십시오

NetApp HWU(Hardware Universe) 애플리케이션은 특정 ONTAP 버전에 대해 지원되는 하드웨어 및 소프트웨어 구성요소를 제공합니다. 현재 ONTAP 소프트웨어가 지원하는 모든 NetApp 스토리지 어플라이언스에 대한 구성 정보를 제공합니다. 구성요소 호환성 표도 제공합니다.

사용하려는 하드웨어 및 소프트웨어 구성 요소가 설치하려는 ONTAP 버전에서 지원되는지 확인합니다.

1. 에 액세스합니다 "HWU" 응용 프로그램 - 시스템 구성 가이드를 봅니다. 컨트롤러 탭을 클릭하여 원하는 사양의 ONTAP 소프트웨어 버전과 NetApp 스토리지 어플라이언스 간의 호환성을 확인하십시오.
2. 또는 스토리지 어플라이언스별로 구성 요소를 비교하려면 스토리지 시스템 비교 를 클릭합니다.

컨트롤러 AFF2XX 시리즈 사전 요구 사항
스토리지 시스템의 물리적 위치를 계획하려면 NetApp Hardware Universe를 참조하십시오. 전기 요구 사항, 지원되는 전원 코드, 온보드 포트 및 케이블 섹션을 참조하십시오.

스토리지 컨트롤러

의 컨트롤러에 대한 물리적 설치 절차를 따릅니다 "AFF A220 문서".

NetApp ONTAP 9.4

구성 워크시트

설치 스크립트를 실행하기 전에 제품 설명서에서 구성 워크시트를 작성하십시오. 구성 워크시트는 에서 사용할 수 있습니다 "ONTAP 9.4 소프트웨어 설정 설명서".

ⓘ 이 시스템은 스위치가 없는 2노드 클러스터 구성에서 설정됩니다.

다음 표에는 ONTAP 9.4 설치 및 구성 정보가 나와 있습니다.

클러스터 세부 정보	클러스터 세부 정보 값입니다
클러스터 노드 A IP 주소입니다	<<var_NodeA_mgmt_ip>> 를 입력합니다
클러스터 노드 A 넷마스크	<<var_NodeA_mgmt_mask>> 를 입력합니다
클러스터 노드 A 게이트웨이	<<var_NodeA_mgmt_gateway>> 를 참조하십시오
클러스터 노드 A 이름	<<var_NodeA>> 를 참조하십시오
클러스터 노드 B IP 주소입니다	<<var_NodeB_mgmt_ip>> 를 입력합니다
클러스터 노드 B 넷마스크	<<var_NodeB_mgmt_mask>> 를 입력합니다

클러스터 세부 정보	클러스터 세부 정보 값입니다
클러스터 노드 B 게이트웨이	<<var_NodeB_mgmt_gateway>> 를 참조하십시오
클러스터 노드 B 이름	<<var_NodeB>> 를 참조하십시오
ONTAP 9.4 URL	<<var_url_boot_software>>
클러스터의 이름입니다	<<var_clustername>> 를 클릭합니다
클러스터 관리 IP 주소입니다	<<var_clustermgmt_ip>> 를 입력합니다
클러스터 B 게이트웨이	<<var_clustermgmt_gateway>> 를 클릭합니다
클러스터 B 넷마스크	<<var_clustermgmt_mask>> 를 입력합니다
도메인 이름	<<var_domain_name>>
DNS 서버 IP(둘 이상 입력할 수 있음)	<<var_dns_server_ip>> 를 참조하십시오
NTP 서버 IP(둘 이상 입력할 수 있음)	<<var_ntp_server_ip>> 를 참조하십시오

노드 **A**를 구성합니다

노드 A를 구성하려면 다음 단계를 완료하십시오.

1. 스토리지 시스템 콘솔 포트에 연결합니다. Loader-A 메시지가 표시됩니다. 하지만 스토리지 시스템이 재부팅 루프 상태인 경우 다음 메시지가 표시될 때 Ctrl-C를 눌러 자동 부팅 루프를 종료합니다.

```
Starting AUTOBOOT press Ctrl-C to abort…
```

2. 시스템이 부팅되도록 합니다.

```
autoboot
```

3. Ctrl-C를 눌러 부팅 메뉴로 들어갑니다.

   ONTAP 9.4가 부팅 중인 소프트웨어 버전이 아닌 경우 다음 단계를 계속하여 새 소프트웨어를 설치합니다. ONTAP 9.4가 부팅 중인 버전인 경우 옵션 8 및 y를 선택하여 노드를 재부팅합니다. 그런 다음 14단계를 계속합니다.

4. 새 소프트웨어를 설치하려면 옵션 '7'을 선택합니다.
5. 업그레이드를 수행하려면 y를 입력하십시오.
6. 다운로드에 사용할 네트워크 포트로 e0M 을 선택합니다.
7. 지금 재부팅하려면 y를 입력하십시오.
8. 각 위치에 e0M의 IP 주소, 넷마스크 및 기본 게이트웨이를 입력합니다.

```
<<var_nodeA_mgmt_ip>> <<var_nodeA_mgmt_mask>> <<var_nodeA_mgmt_gateway>>
```

9. 소프트웨어를 찾을 수 있는 URL을 입력합니다.

이 웹 서버는 Ping할 수 있어야 합니다.

```
<<var_url_boot_software>>
```

10. 사용자 이름에 대해 Enter 키를 눌러 사용자 이름이 없음을 나타냅니다.
11. 새로 설치한 소프트웨어를 이후 재부팅에 사용할 기본값으로 설정하려면 'y'를 입력합니다.
12. 노드를 재부팅하려면 y를 입력합니다.

    새 소프트웨어를 설치할 때 시스템이 BIOS 및 어댑터 카드에 대한 펌웨어 업그레이드를 수행할 수 있으며, 이로 인해 LOADER-A 프롬프트에서 재부팅되고 중지될 수 있습니다. 이러한 작업이 발생하면 시스템이 이 절차를 벗어날 수 있습니다.

13. Ctrl-C를 눌러 부팅 메뉴로 들어갑니다.
14. Clean Configuration 및 Initialize All Disks 옵션을 4로 선택합니다.
15. 디스크를 제로화하려면 y를 입력하고 구성을 재설정한 다음 새 파일 시스템을 설치합니다.
16. 디스크에 있는 모든 데이터를 지우려면 'y'를 입력합니다.

    연결된 디스크의 수와 유형에 따라 루트 애그리게이트의 초기화 및 생성을 완료하는 데 90분 이상이 걸릴 수 있습니다. 초기화가 완료되면 스토리지 시스템이 재부팅됩니다. SSD를 초기화하는 데 걸리는 시간은 상당히 줄어듭니다. 노드 A용 디스크가 제로화하는 동안 노드 B 구성을 계속할 수 있습니다.

17. 노드 A를 초기화하는 동안 노드 B를 구성합니다

노드 **B**를 구성합니다

노드 B를 구성하려면 다음 단계를 완료하십시오.

1. 스토리지 시스템 콘솔 포트에 연결합니다. Loader-A 메시지가 표시됩니다. 하지만 스토리지 시스템이 재부팅 루프 상태인 경우 다음 메시지가 표시될 때 Ctrl-C를 눌러 자동 부팅 루프를 종료합니다.

```
Starting AUTOBOOT press Ctrl-C to abort…
```

2. Ctrl-C를 눌러 부팅 메뉴로 들어갑니다.

```
autoboot
```

3. 메시지가 나타나면 Ctrl-C를 누릅니다.

    ONTAP 9.4가 부팅 중인 소프트웨어 버전이 아닌 경우 다음 단계를 계속하여 새 소프트웨어를 설치합니다. ONTAP 9.4가 부팅 중인 버전인 경우 옵션 8 및 y를 선택하여 노드를 재부팅합니다. 그런 다음 14단계를 계속합니다.

4. 새 소프트웨어를 설치하려면 옵션 7을 선택합니다.
5. 업그레이드를 수행하려면 y를 입력하십시오.

6. 다운로드에 사용할 네트워크 포트로 e0M 을 선택합니다.
7. 지금 재부팅하려면 y를 입력하십시오.
8. 각 위치에 e0M의 IP 주소, 넷마스크 및 기본 게이트웨이를 입력합니다.

```
<<var_nodeB_mgmt_ip>> <<var_nodeB_mgmt_ip>><<var_nodeB_mgmt_gateway>>
```

9. 소프트웨어를 찾을 수 있는 URL을 입력합니다.

   이 웹 서버는 Ping할 수 있어야 합니다.

```
<<var_url_boot_software>>
```

10. 사용자 이름에 대해 Enter 키를 눌러 사용자 이름이 없음을 나타냅니다.
11. 새로 설치한 소프트웨어를 이후 재부팅에 사용할 기본값으로 설정하려면 'y'를 입력합니다.
12. 노드를 재부팅하려면 y를 입력합니다.

    새 소프트웨어를 설치할 때 시스템이 BIOS 및 어댑터 카드에 대한 펌웨어 업그레이드를 수행할 수 있으며, 이로 인해 LOADER-A 프롬프트에서 재부팅되고 중지될 수 있습니다. 이러한 작업이 발생하면 시스템이 이 절차를 벗어날 수 있습니다.

13. Ctrl-C를 눌러 부팅 메뉴로 들어갑니다.
14. Clean Configuration(구성 정리) 및 Initialize All Disks(모든 디스크 초기화) 에 대해 옵션 4 를 선택합니다.
15. 디스크를 제로화하려면 y를 입력하고 구성을 재설정한 다음 새 파일 시스템을 설치합니다.
16. 디스크에 있는 모든 데이터를 지우려면 'y'를 입력합니다.

    연결된 디스크의 수와 유형에 따라 루트 애그리게이트의 초기화 및 생성을 완료하는 데 90분 이상이 걸릴 수 있습니다. 초기화가 완료되면 스토리지 시스템이 재부팅됩니다. SSD를 초기화하는 데 걸리는 시간은 상당히 줄어듭니다.

노드 **A** 구성 및 클러스터 구성 계속

스토리지 컨트롤러 A(노드 A) 콘솔 포트에 연결된 콘솔 포트 프로그램에서 노드 설정 스크립트를 실행합니다. 이 스크립트는 ONTAP 9.4가 노드에서 처음 부팅될 때 나타납니다.

ONTAP 9.4에서 노드 및 클러스터 설정 절차가 약간 변경되었습니다. 이제 클러스터 설정 마법사를 사용하여 클러스터의 첫 번째 노드를 구성하고 System Manager를 사용하여 클러스터를 구성할 수 있습니다.

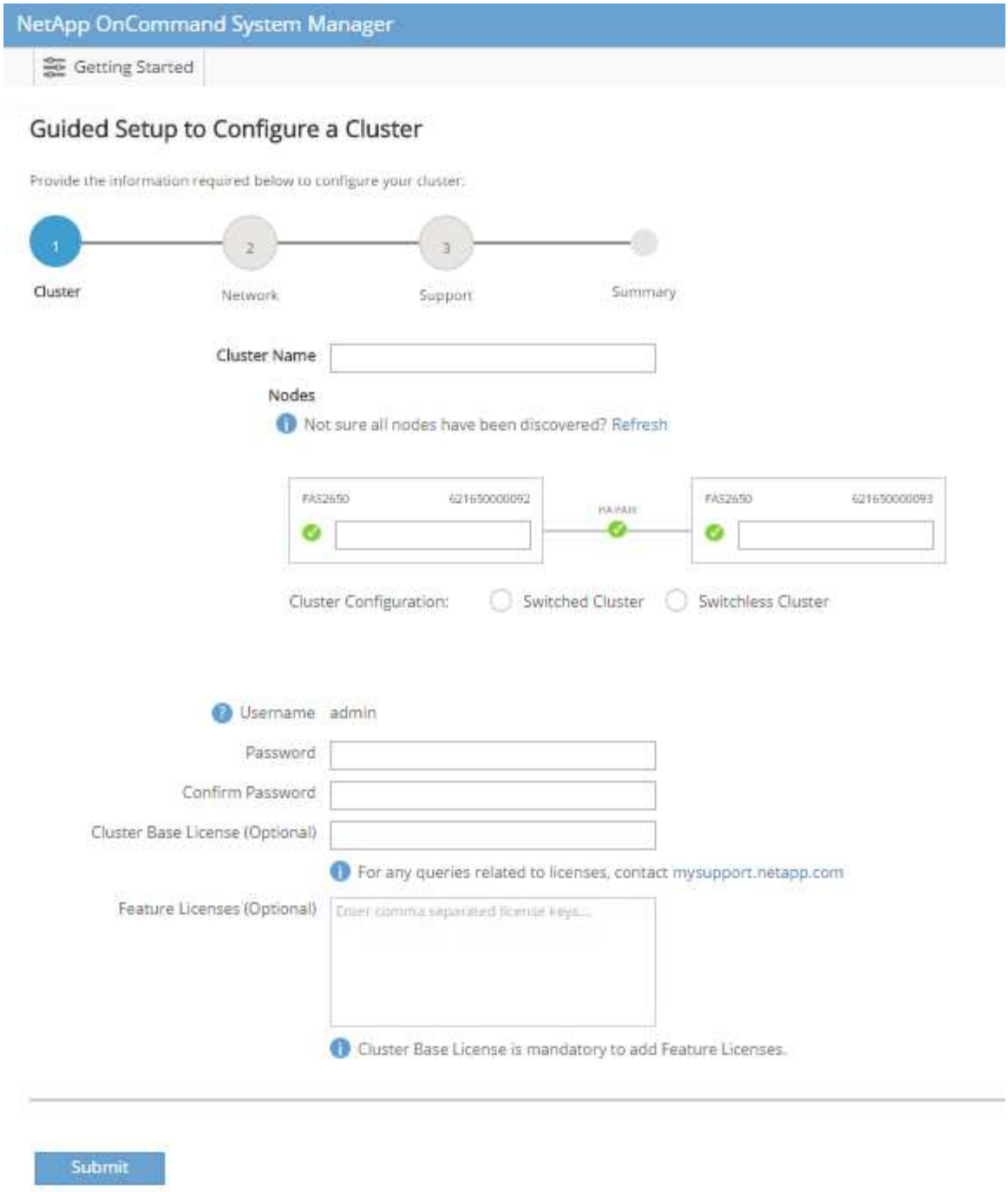
1. 프롬프트에 따라 노드 A를 설정합니다

```
Welcome to the cluster setup wizard.
You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the cluster setup wizard.
     Any changes you made before quitting will be saved.
You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value.
This system will send event messages and periodic reports to NetApp
Technical
Support. To disable this feature, enter
autosupport modify -support disable
within 24 hours.
Enabling AutoSupport can significantly speed problem determination and
resolution should a problem occur on your system.
For further information on AutoSupport, see:
http://support.netapp.com/autosupport/
Type yes to confirm and continue {yes}: yes
Enter the node management interface port [e0M]:
Enter the node management interface IP address: <<var_nodeA_mgmt_ip>>
Enter the node management interface netmask: <<var_nodeA_mgmt_mask>>
Enter the node management interface default gateway:
<<var_nodeA_mgmt_gateway>>
A node management interface on port e0M with IP address
<<var_nodeA_mgmt_ip>> has been created.
Use your web browser to complete cluster setup by accessing
https://<<var_nodeA_mgmt_ip>>
Otherwise, press Enter to complete cluster setup using the command line
interface:
```

2. 노드의 관리 인터페이스의 IP 주소로 이동합니다.

   CLI를 사용하여 클러스터를 설정할 수도 있습니다. 이 문서에서는 NetApp System Manager의 안내에 따라 설정을 사용하는 클러스터 설정에 대해 설명합니다.

3. Guided Setup(안내식 설정) 을 클릭하여 클러스터를 구성합니다.
4. 클러스터 이름은 <<var_clustername>>'을, 구성 중인 각 노드에 대해서는 <<var_NodeA>>'와 <<var_NodeB>>를 입력합니다. 스토리지 시스템에 사용할 암호를 입력합니다. 클러스터 유형으로 Switchless Cluster를 선택합니다. 클러스터 기본 라이센스를 입력합니다.



5. 클러스터, NFS 및 iSCSI에 대한 기능 라이센스도 입력할 수 있습니다.
6. 클러스터를 생성 중임을 나타내는 상태 메시지가 표시됩니다. 이 상태 메시지는 여러 상태를 순환합니다. 이 과정은 몇 분 정도 소요됩니다.
7. 네트워크를 구성합니다.
   a. IP 주소 범위 옵션을 선택 취소합니다.
   b. Cluster Management IP Address 필드(<<var_clustermgmt_ip>>)에 넷마스크 필드(<<var_clustermgmt_mask>>)에 <<var_clustermgmt_gateway>>)를 입력합니다. 다음을 사용하십시오. 포트 필드의 선택기로 노드 A의 e0M을 선택합니다
   c. 노드 A의 노드 관리 IP가 이미 채워져 있습니다. 노드 B에 대해 '<<var_NodeA_mgmt_ip>>'를 입력합니다

d. DNS Domain Name 필드에 '<<var_domain_name>>'을 입력합니다. DNS 서버 IP 주소 필드에 '<<var_dns_server_ip>>'를 입력합니다.

   여러 DNS 서버 IP 주소를 입력할 수 있습니다.

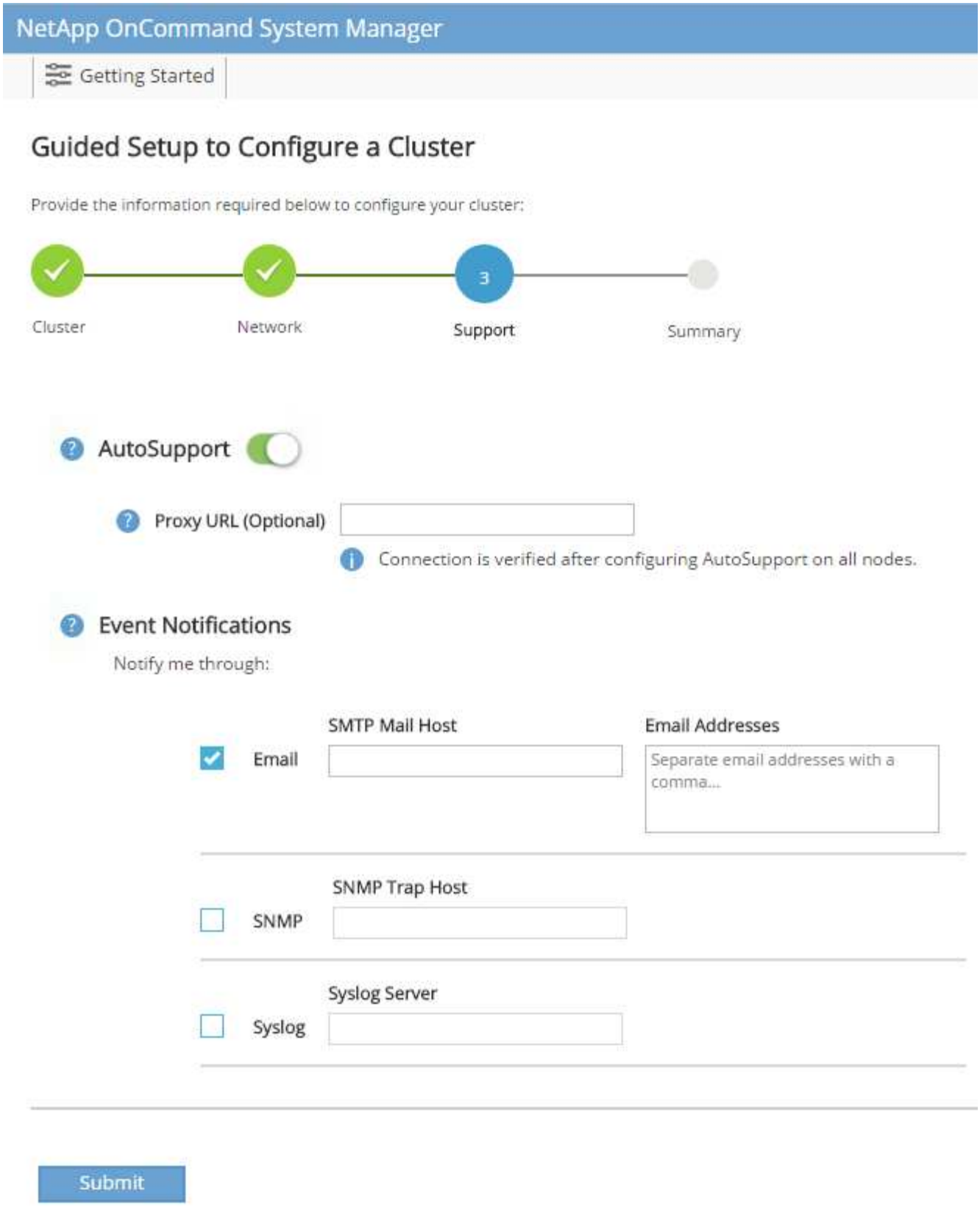
e. Primary NTP Server 필드에 '<<var_ntp_server_ip>>'를 입력합니다.

   대체 NTP 서버를 입력할 수도 있습니다.

8. 지원 정보를 구성합니다.

   a. 환경에 AutoSupport에 액세스하기 위한 프록시가 필요한 경우 프록시 URL에 URL을 입력합니다.
   b. 이벤트 알림에 대한 SMTP 메일 호스트 및 이메일 주소를 입력합니다.

      계속하려면 이벤트 알림 방법을 설정해야 합니다. 방법 중 하나를 선택할 수 있습니다.



9. 클러스터 구성이 완료되었으면 클러스터 관리 를 클릭하여 스토리지를 구성합니다.

스토리지 노드 및 기본 클러스터를 구성한 후에는 스토리지 클러스터 구성을 계속할 수 있습니다.

모든 스페어 디스크를 제로합니다

클러스터의 모든 스페어 디스크를 제로하려면 다음 명령을 실행합니다.

```
disk zerospares
```

온보드 **UTA2** 포트 속성을 설정합니다

1. ucadmin show 명령을 실행하여 현재 모드와 포트의 현재 유형을 확인합니다.

```
AFF A220::> ucadmin show
                     Current  Current    Pending  Pending    Admin
Node          Adapter  Mode     Type       Mode     Type       Status
------------  -------  -------  ---------  -------  ---------
-----------
AFF A220_A     0c       fc       target     -        -          online
AFF A220_A     0d       fc       target     -        -          online
AFF A220_A     0e       fc       target     -        -          online
AFF A220_A     0f       fc       target     -        -          online
AFF A220_B     0c       fc       target     -        -          online
AFF A220_B     0d       fc       target     -        -          online
AFF A220_B     0e       fc       target     -        -          online
AFF A220_B     0f       fc       target     -        -          online
8 entries were displayed.
```

2. 사용 중인 포트의 현재 모드가 CNA인지, 현재 유형이 'target'으로 설정되어 있는지 확인합니다. 그렇지 않은 경우 다음 명령을 사용하여 포트 속성을 변경합니다.

```
ucadmin modify -node <home node of the port> -adapter <port name> -mode
cna -type target
```

이전 명령을 실행하려면 포트가 오프라인 상태여야 합니다. 포트를 오프라인으로 전환하려면 다음 명령을 실행합니다.

```
`network fcp adapter modify -node <home node of the port> -adapter <port
name> -state down`
```

포트 속성을 변경한 경우 변경 사항을 적용하려면 각 노드를 재부팅해야 합니다.

관리 논리 인터페이스(**LIF**) 이름 바꾸기

관리 LIF의 이름을 변경하려면 다음 단계를 수행하십시오.

1. 현재 관리 LIF 이름을 표시합니다.

```
network interface show –vserver <<clustername>>
```

2. 클러스터 관리 LIF의 이름을 바꿉니다.

```
network interface rename –vserver <<clustername>> –lif
cluster_setup_cluster_mgmt_lif_1 –newname cluster_mgmt
```

3. 노드 B 관리 LIF의 이름을 바꿉니다.

```
network interface rename -vserver <<clustername>> -lif
cluster_setup_node_mgmt_lif_AFF A220_B_1 -newname AFF A220-02_mgmt1
```

클러스터 관리에서 자동 되돌리기 설정

클러스터 관리 인터페이스에서 자동 되돌리기 매개 변수를 설정합니다.

```
network interface modify –vserver <<clustername>> -lif cluster_mgmt –auto-
revert true
```

서비스 프로세서 네트워크 인터페이스를 설정합니다

각 노드의 서비스 프로세서에 정적 IPv4 주소를 할당하려면 다음 명령을 실행합니다.

```
system service-processor network modify –node <<var_nodeA>> -address
-family IPv4 –enable true –dhcp none –ip-address <<var_nodeA_sp_ip>>
-netmask <<var_nodeA_sp_mask>> -gateway <<var_nodeA_sp_gateway>>
system service-processor network modify –node <<var_nodeB>> -address
-family IPv4 –enable true –dhcp none –ip-address <<var_nodeB_sp_ip>>
-netmask <<var_nodeB_sp_mask>> -gateway <<var_nodeB_sp_gateway>>
```

ⓘ 서비스 프로세서 IP 주소는 노드 관리 IP 주소와 동일한 서브넷에 있어야 합니다.

ONTAP에서 스토리지 페일오버 설정

스토리지 페일오버가 설정되었는지 확인하려면 페일오버 쌍에서 다음 명령을 실행합니다.

1. 스토리지 페일오버 상태를 확인합니다.

```
storage failover show
```

'<<var_NodeA>>'와 '<<var_NodeB>>'는 모두 테이크오버를 수행할 수 있어야 합니다. 노드가 테이크오버 수행 가능한 경우 3단계로 이동하십시오.

2. 두 노드 중 하나에서 페일오버가 사용되도록 설정합니다.

```
storage failover modify -node <<var_nodeA>> -enabled true
```

한 노드에서 페일오버가 사용되도록 설정하면 두 노드 모두에서 설정됩니다.

3. 2노드 클러스터의 HA 상태를 확인합니다.

2개 이상의 노드가 있는 클러스터에는 이 단계를 적용할 수 없습니다.

```
cluster ha show
```

4. 고가용성이 구성된 경우 6단계로 이동합니다. 고가용성이 구성된 경우 명령을 실행하면 다음 메시지가 표시됩니다.

```
High Availability Configured: true
```

5. 2노드 클러스터에만 HA 모드를 사용하도록 설정합니다.

> ⓘ 2개 이상의 노드가 있는 클러스터에서는 페일오버에 문제가 발생하므로 이 명령을 실행하지 마십시오.

```
cluster ha modify -configured true
Do you want to continue? {y|n}: y
```

6. 하드웨어 지원이 올바르게 구성되어 있는지 확인하고 필요한 경우 파트너 IP 주소를 수정합니다.

```
storage failover hwassist show
```

"Keep Alive Status: Error: whwassist keep alive alert from partner(활성 상태 유지: 오류: 파트너의 hwassist keep alive 경고를 수신하지 못했습니다)" 메시지는 하드웨어 지원이 구성되지 않았음을 나타냅니다. 다음 명령을 실행하여 하드웨어 지원을 구성합니다.

```
storage failover modify –hwassist-partner-ip <<var_nodeB_mgmt_ip>> -node
<<var_nodeA>>
storage failover modify –hwassist-partner-ip <<var_nodeA_mgmt_ip>> -node
<<var_nodeB>>
```

ONTAP에서 점보 프레임 **MTU** 브로드캐스트 도메인을 생성합니다

MTU가 9000인 데이터 브로드캐스트 도메인을 생성하려면 다음 명령을 실행합니다.

```
broadcast-domain create -broadcast-domain Infra_NFS -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-A -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-B -mtu 9000
```

기본 브로드캐스트 도메인에서 데이터 포트를 제거합니다

10GbE 데이터 포트는 iSCSI/NFS 트래픽에 사용되며 이러한 포트는 기본 도메인에서 제거해야 합니다. 포트 e0e 및 e0f는 사용되지 않으며 기본 도메인에서도 제거해야 합니다.

브로드캐스트 도메인에서 포트를 제거하려면 다음 명령을 실행합니다.

```
broadcast-domain remove-ports -broadcast-domain Default -ports
<<var_nodeA>>:e0c, <<var_nodeA>>:e0d, <<var_nodeA>>:e0e,
<<var_nodeA>>:e0f, <<var_nodeB>>:e0c, <<var_nodeB>>:e0d,
<<var_nodeA>>:e0e, <<var_nodeA>>:e0f
```

UTA2 포트에서 흐름 제어를 사용하지 않도록 설정합니다

외부 장치에 연결된 모든 UTA2 포트에서 흐름 제어를 사용하지 않도록 설정하는 것이 NetApp의 모범 사례입니다. 흐름 제어를 사용하지 않도록 설정하려면 다음 명령을 실행합니다.

```
net port modify -node <<var_nodeA>> -port e0c -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0d -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0e -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0f -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0c -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0d -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0e -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0f -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
```

ONTAP에서 **IFGRP LACP**를 구성합니다

이 인터페이스 그룹 유형에 2개 이상의 이더넷 인터페이스와 LACP를 지원하는 스위치가 필요합니다. 스위치가 올바르게 구성되었는지 확인합니다.

클러스터 프롬프트에서 다음 단계를 완료합니다.

```
ifgrp create -node <<var_nodeA>> -ifgrp a0a -distr-func port -mode
multimode_lacp
network port ifgrp add-port -node <<var_nodeA>> -ifgrp a0a -port e0c
network port ifgrp add-port -node <<var_nodeA>> -ifgrp a0a -port e0d
ifgrp create -node << var_nodeB>> -ifgrp a0a -distr-func port -mode
multimode_lacp
network port ifgrp add-port -node <<var_nodeB>> -ifgrp a0a -port e0c
network port ifgrp add-port -node <<var_nodeB>> -ifgrp a0a -port e0d
```

NetApp ONTAP에서 점보 프레임을 구성합니다

ONTAP 네트워크 포트에서 점보 프레임(일반적으로 9,000바이트 MTU 사용)을 사용하도록 구성하려면 클러스터 쉘에서 다음 명령을 실행합니다.

```
AFF A220::> network port modify -node node_A -port a0a -mtu 9000
Warning: This command will cause a several second interruption of service
on
         this network port.
Do you want to continue? {y|n}: y
AFF A220::> network port modify -node node_B -port a0a -mtu 9000
Warning: This command will cause a several second interruption of service
on
         this network port.
Do you want to continue? {y|n}: y
```

ONTAP에서 **VLAN**을 생성합니다

ONTAP에서 VLAN을 생성하려면 다음 단계를 수행하십시오.

1. NFS VLAN 포트를 생성하여 데이터 브로드캐스트 도메인에 추가합니다.

```
network port vlan create –node <<var_nodeA>> -vlan-name a0a-
<<var_nfs_vlan_id>>
network port vlan create –node <<var_nodeB>> -vlan-name a0a-
<<var_nfs_vlan_id>>
broadcast-domain add-ports -broadcast-domain Infra_NFS -ports
<<var_nodeA>>:a0a-<<var_nfs_vlan_id>>, <<var_nodeB>>:a0a-
<<var_nfs_vlan_id>>
```

2. iSCSI VLAN 포트를 생성하여 데이터 브로드캐스트 도메인에 추가합니다.

```
network port vlan create –node <<var_nodeA>> -vlan-name a0a-
<<var_iscsi_vlan_A_id>>
network port vlan create –node <<var_nodeA>> -vlan-name a0a-
<<var_iscsi_vlan_B_id>>
network port vlan create –node <<var_nodeB>> -vlan-name a0a-
<<var_iscsi_vlan_A_id>>
network port vlan create –node <<var_nodeB>> -vlan-name a0a-
<<var_iscsi_vlan_B_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-A -ports
<<var_nodeA>>:a0a-<<var_iscsi_vlan_A_id>>, <<var_nodeB>>:a0a-
<<var_iscsi_vlan_A_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-B -ports
<<var_nodeA>>:a0a-<<var_iscsi_vlan_B_id>>, <<var_nodeB>>:a0a-
<<var_iscsi_vlan_B_id>>
```

3. MGMT-VLAN 포트를 생성합니다.

```
network port vlan create –node <<var_nodeA>> -vlan-name a0a-
<<mgmt_vlan_id>>
network port vlan create –node <<var_nodeB>> -vlan-name a0a-
<<mgmt_vlan_id>>
```

ONTAP에서 애그리게이트를 생성합니다

ONTAP 설정 프로세스 중에 루트 볼륨이 포함된 애그리게이트가 생성됩니다. 추가 애그리게이트를 생성하려면 애그리게이트 이름, 애그리게이트를 생성할 노드, 애그리게이트에 포함된 디스크 수를 결정합니다.

Aggregate를 생성하려면 다음 명령을 실행합니다.

```
aggr create -aggregate aggr1_nodeA -node <<var_nodeA>> -diskcount
<<var_num_disks>>
aggr create -aggregate aggr1_nodeB -node <<var_nodeB>> -diskcount
<<var_num_disks>>
```

구성에 최소 하나의 디스크(가장 큰 디스크 선택)를 스페어로 보관합니다. 모범 사례는 각 디스크 유형 및 크기에 대해 하나 이상의 스페어를 두는 것입니다.

5개의 디스크로 시작합니다. 스토리지를 추가해야 할 때 디스크를 애그리게이트에 추가할 수 있습니다.

디스크 비우기가 완료될 때까지 애그리게이트를 생성할 수 없습니다. 집계 생성 상태를 표시하려면 'aggr show' 명령을 실행합니다. aggr1 _ NodeA가 온라인이 될 때까지 진행하지 마십시오.

ONTAP에서 시간대를 구성합니다

시간 동기화를 구성하고 클러스터에서 표준 시간대를 설정하려면 다음 명령을 실행합니다.

```
timezone <<var_timezone>>
```

예를 들어 미국 동부의 시간대는 미국/뉴욕입니다. 표준 시간대 이름을 입력하기 시작하면 Tab 키를 눌러 사용 가능한 옵션을 확인합니다.

ONTAP에서 SNMP를 구성합니다

SNMP를 구성하려면 다음 단계를 수행하십시오.

1. 위치 및 연락처와 같은 SNMP 기본 정보를 구성합니다. 이 정보는 SNMP에서 'SysLocation', 'SysContact' 변수로 표시됩니다.

```
snmp contact <<var_snmp_contact>>
snmp location "<<var_snmp_location>>"
snmp init 1
options snmp.enable on
```

2. 원격 호스트에 보낼 SNMP 트랩을 구성합니다.

```
snmp traphost add <<var_snmp_server_fqdn>>
```

ONTAP에서 SNMPv1을 구성합니다

SNMPv1을 구성하려면 커뮤니티라는 공유 암호 일반 텍스트 암호를 설정합니다.

```
snmp community add ro <<var_snmp_community>>
```

NMP community delete all 명령을 주의하여 사용한다. 다른 모니터링 제품에 커뮤니티 문자열을 사용하는 경우 이 명령은 해당 문자열을 제거합니다.

ONTAP에서 SNMPv3을 구성합니다

SNMPv3을 사용하려면 인증을 위해 사용자를 정의하고 구성해야 합니다. SNMPv3을 구성하려면 다음 단계를 수행하십시오.

1. Security snmpusers 명령을 실행하여 엔진 ID를 조회한다.
2. 'snmpv3user'라는 사용자를 생성합니다.

```
security login create -username snmpv3user -authmethod usm -application
snmp
```

3. 신뢰할 수 있는 엔터티의 엔진 ID를 입력하고 인증 프로토콜로 md5 를 선택한다.
4. 메시지가 나타나면 인증 프로토콜에 사용할 최소 길이 8자로 된 암호를 입력합니다.
5. 개인 정보 보호 프로토콜로 'des'를 선택합니다.
6. 메시지가 나타나면 개인 정보 보호 프로토콜에 사용할 최소 길이 8자로 된 암호를 입력합니다.

ONTAP에서 **AutoSupport HTTPS**를 구성합니다

NetApp AutoSupport 툴은 HTTPS를 통해 지원 요약 정보를 NetApp에 보냅니다. AutoSupport를 구성하려면 다음 명령을 실행합니다.

```
system node autosupport modify -node * -state enable –mail-hosts
<<var_mailhost>> -transport https -support enable -noteto
<<var_storage_admin_email>>
```

스토리지 가상 머신을 생성합니다

인프라 스토리지 가상 시스템(SVM)을 생성하려면 다음 단계를 완료하십시오.

1. 'vserver create' 명령을 실행합니다.

```
vserver create –vserver Infra-SVM –rootvolume rootvol –aggregate
aggr1_nodeA –rootvolume-security-style unix
```

2. NetApp VSC를 위한 인프라-SVM 애그리게이트 목록에 데이터 애그리게이트를 추가합니다.

```
vserver modify -vserver Infra-SVM -aggr-list aggr1_nodeA,aggr1_nodeB
```

3. NFS와 iSCSI를 남겨두고 SVM에서 사용하지 않는 스토리지 프로토콜을 제거합니다.

```
vserver remove-protocols –vserver Infra-SVM -protocols cifs,ndmp,fcp
```

4. 인프라 SVM에서 NFS 프로토콜을 사용하고 실행합니다.

```
`nfs create -vserver Infra-SVM -udp disabled`
```

5. NetApp NFS VAAI 플러그인에 대한 'VM vStorage' 매개 변수를 설정합니다. 그런 다음 NFS가 구성되었는지 확인합니다.

```
`vserver nfs modify –vserver Infra-SVM –vstorage enabled`
`vserver nfs show `
```

스토리지 가상 시스템이 이전에 서버라고 불리기 때문에 명령줄에서는 'vserver'가 명령을 앞에 표시합니다.

ONTAP에서 **NFSv3**을 구성합니다

다음 표에는 이 구성을 완료하는 데 필요한 정보가 나와 있습니다.

세부 정보	상세 값
ESXi 호스트 NFS IP 주소입니다	<<var_esxi_hostA_nfs_ip>> 를 참조하십시오
ESXi 호스트 B NFS IP 주소입니다	<<var_esxi_hostB_nfs_ip>> 를 참조하십시오

SVM에서 NFS를 구성하려면 다음 명령을 실행합니다.

1. 기본 엑스포트 정책에서 각 ESXi 호스트에 대한 규칙을 생성합니다.
2. 생성 중인 각 ESXi 호스트에 대해 규칙을 할당합니다. 각 호스트에는 고유한 규칙 인덱스가 있습니다. 첫 번째 ESXi 호스트에는 규칙 인덱스 1이 있고 두 번째 ESXi 호스트에는 규칙 인덱스 2가 있습니다.

```
vserver export-policy rule create –vserver Infra-SVM -policyname default
–ruleindex 1 –protocol nfs -clientmatch <<var_esxi_hostA_nfs_ip>>
-rorule sys –rwrule sys -superuser sys –allow-suid false
vserver export-policy rule create –vserver Infra-SVM -policyname default
–ruleindex 2 –protocol nfs -clientmatch <<var_esxi_hostB_nfs_ip>>
-rorule sys –rwrule sys -superuser sys –allow-suid false
vserver export-policy rule show
```

3. 인프라 SVM 루트 볼륨에 엑스포트 정책을 할당합니다.

```
volume modify –vserver Infra-SVM –volume rootvol –policy default
```

vSphere를 설정한 후 NetApp VSC는 엑스포트 정책을 자동으로 처리합니다. 설치하지 않은 경우 Cisco UCS C-Series 서버를 추가할 때 엑스포트 정책 규칙을 생성해야 합니다.

ONTAP에서 **iSCSI** 서비스를 생성합니다

iSCSI 서비스를 생성하려면 다음 단계를 완료하십시오.

1. SVM에서 iSCSI 서비스를 생성합니다. 또한 이 명령은 iSCSI 서비스를 시작하고 SVM에 대한 iSCSI IQN을 설정합니다. iSCSI가 구성되었는지 확인합니다.

```
iscsi create -vserver Infra-SVM
iscsi show
```

ONTAP에서 **SVM** 루트 볼륨의 로드 공유 미러를 생성합니다

1. 각 노드에서 인프라 SVM 루트 볼륨의 로드 공유 미러가 될 볼륨을 생성합니다.

```
volume create –vserver Infra_Vserver –volume rootvol_m01 –aggregate
aggr1_nodeA –size 1GB –type DP
volume create –vserver Infra_Vserver –volume rootvol_m02 –aggregate
aggr1_nodeB –size 1GB –type DP
```

2. 15분마다 루트 볼륨 미러 관계를 업데이트하는 작업 스케줄을 생성합니다.

```
job schedule interval create -name 15min -minutes 15
```

3. 미러링 관계를 생성합니다.

```
snapmirror create -source-path Infra-SVM:rootvol -destination-path
Infra-SVM:rootvol_m01 -type LS -schedule 15min
snapmirror create -source-path Infra-SVM:rootvol -destination-path
Infra-SVM:rootvol_m02 -type LS -schedule 15min
```

4. 미러링 관계를 초기화하고 미러링 관계가 만들어졌는지 확인합니다.

```
snapmirror initialize-ls-set -source-path Infra-SVM:rootvol
snapmirror show
```

ONTAP에서 **HTTPS** 액세스를 구성합니다

스토리지 컨트롤러에 대한 보안 액세스를 구성하려면 다음 단계를 수행하십시오.

1. 인증서 명령에 액세스할 수 있도록 권한 수준을 높입니다.

```
set -privilege diag
Do you want to continue? {y|n}: y
```

2. 일반적으로 자체 서명된 인증서가 이미 있습니다. 다음 명령을 실행하여 인증서를 확인합니다.

```
security certificate show
```

3. 표시된 각 SVM에서 인증서 공통 이름은 SVM의 DNS FQDN과 일치해야 합니다. 네 개의 기본 인증서를 삭제하고 자체 서명된 인증서 또는 인증 기관의 인증서로 대체해야 합니다.

   인증서를 만들기 전에 만료된 인증서를 삭제하는 것이 좋습니다. 만료된 인증서를 삭제하려면 보안 인증서 삭제 명령을 실행합니다. 다음 명령에서 Tab completion을 사용하여 각 기본 인증서를 선택하고 삭제합니다.

```
security certificate delete [TAB] …
Example: security certificate delete -vserver Infra-SVM -common-name
Infra-SVM -ca Infra-SVM -type server -serial 552429A6
```

4. 자체 서명된 인증서를 생성하고 설치하려면 다음 명령을 일회성 명령으로 실행합니다. 인프라 SVM 및 클러스터 SVM에 대한 서버 인증서를 생성합니다. 다시 한 번 탭 완료 기능을 사용하면 이러한 명령을 쉽게 완료할 수 있습니다.

```
security certificate create [TAB] …
Example: security certificate create -common-name infra-svm. netapp.com
-type  server -size 2048 -country US -state "North Carolina" -locality
"RTP" -organization "NetApp" -unit "FlexPod" -email-addr
"abc@netapp.com" -expire-days 365 -protocol SSL -hash-function SHA256
-vserver Infra-SVM
```

5. 다음 단계에서 필요한 매개 변수 값을 얻으려면 'security certificate show' 명령을 실행합니다.
6. '–server-enabled true' 및 '–client-enabled false' 매개 변수를 사용하여 방금 만든 각 인증서를 활성화합니다. 다시 탭 완료를 사용합니다.

```
security ssl modify [TAB] …
Example: security ssl modify -vserver Infra-SVM -server-enabled true
-client-enabled false -ca infra-svm.netapp.com -serial 55243646 -common
-name infra-svm.netapp.com
```

7. SSL 및 HTTPS 액세스를 구성 및 활성화하고 HTTP 액세스를 비활성화합니다.

```
system services web modify -external true -sslv3-enabled true
Warning: Modifying the cluster configuration will cause pending web
service requests to be
         interrupted as the web servers are restarted.
Do you want to continue {y|n}: y
system services firewall policy delete -policy mgmt -service http
–vserver <<var_clustername>>
```

명령 실행 중 일부에서 항목이 존재하지 않는다는 오류 메시지가 반환되는 것은 정상입니다.

8. 관리 권한 수준으로 되돌아가며 SVM을 웹에서 사용할 수 있도록 설정을 생성합니다.

```
set -privilege admin
vserver services web modify -name spi|ontapi|compat -vserver * -enabled
true
```

ONTAP에서 **NetApp FlexVol** 볼륨을 생성합니다

NetApp FlexVol 볼륨을 생성하려면 볼륨 이름, 크기 및 이 볼륨이 있는 애그리게이트를 입력합니다. 2개의 VMware 데이터 저장소 볼륨과 서버 부팅 볼륨을 생성합니다.

```
volume create -vserver Infra-SVM -volume infra_datastore_1 -aggregate
aggr1_nodeA -size 500GB -state online -policy default -junction-path
/infra_datastore_1 -space-guarantee none -percent-snapshot-space 0
volume create -vserver Infra-SVM -volume infra_swap -aggregate aggr1_nodeA
-size 100GB -state online -policy default -junction-path /infra_swap
-space-guarantee none -percent-snapshot-space 0 -snapshot-policy none
volume create -vserver Infra-SVM -volume esxi_boot -aggregate aggr1_nodeA
-size 100GB -state online -policy default -space-guarantee none -percent
-snapshot-space 0
```

ONTAP에서 중복 제거를 설정합니다

적절한 볼륨에서 중복 제거를 설정하려면 다음 명령을 실행합니다.

```
volume efficiency on -vserver Infra-SVM -volume infra_datastore_1
volume efficiency on -vserver Infra-SVM -volume esxi_boot
```

ONTAP에서 **LUN**을 생성합니다

2개의 부팅 LUN을 생성하려면 다음 명령을 실행합니다.

```
lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-A -size
15GB -ostype vmware -space-reserve disabled
lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-B -size
15GB -ostype vmware -space-reserve disabled
```

Cisco UCS C-Series 서버를 더 추가할 때는 부팅 LUN을 더 생성해야 합니다.

ONTAP에서 iSCSI LIF를 생성합니다

다음 표에는 이 구성을 완료하는 데 필요한 정보가 나와 있습니다.

세부 정보	상세 값
스토리지 노드 A iSCSI LIF01A	<<var_NodeA_iscsi_lif01a_ip>> 를 참조하십시오
스토리지 노드 A iSCSI LIF01A 네트워크 마스크입니다	<<var_NodeA_iscsi_lif01a_mask>>
스토리지 노드 A iSCSI LIF01B	<<var_NodeA_iscsi_liff 01b_ip>> 를 참조하십시오
스토리지 노드 A iSCSI LIF01B 네트워크 마스크입니다	<<var_NodeA_iscsi_liff 01b_mask>>
스토리지 노드 B iSCSI LIF01A	<<var_NodeB_iscsi_liff 01a_ip>>
스토리지 노드 B iSCSI LIF01A 네트워크 마스크입니다	<<var_NodeB_iscsi_liff 01a_mask>>
스토리지 노드 B iSCSI LIF01B	<<var_NodeB_iscsi_liff 01b_ip>>
스토리지 노드 B iSCSI LIF01B 네트워크 마스크입니다	<<var_NodeB_iscsi_liff 01b_mask>>

1. 각 노드에 2개의 iSCSI LIF를 4개 생성합니다.

```
network interface create -vserver Infra-SVM -lif iscsi_lif01a -role data
-data-protocol iscsi -home-node <<var_nodeA>> -home-port a0a-
<<var_iscsi_vlan_A_id>> -address <<var_nodeA_iscsi_lif01a_ip>> -netmask
<<var_nodeA_iscsi_lif01a_mask>> –status-admin up –failover-policy
disabled –firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif01b -role data
-data-protocol iscsi -home-node <<var_nodeA>> -home-port a0a-
<<var_iscsi_vlan_B_id>> -address <<var_nodeA_iscsi_lif01b_ip>> -netmask
<<var_nodeA_iscsi_lif01b_mask>> –status-admin up –failover-policy
disabled –firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02a -role data
-data-protocol iscsi -home-node <<var_nodeB>> -home-port a0a-
<<var_iscsi_vlan_A_id>> -address <<var_nodeB_iscsi_lif01a_ip>> -netmask
<<var_nodeB_iscsi_lif01a_mask>> –status-admin up –failover-policy
disabled –firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02b -role data
-data-protocol iscsi -home-node <<var_nodeB>> -home-port a0a-
<<var_iscsi_vlan_B_id>> -address <<var_nodeB_iscsi_lif01b_ip>> -netmask
<<var_nodeB_iscsi_lif01b_mask>> –status-admin up –failover-policy
disabled –firewall-policy data –auto-revert false
network interface show
```

ONTAP에서 NFS LIF를 생성합니다

다음 표에는 이 구성을 완료하는 데 필요한 정보가 나와 있습니다.

세부 정보	상세 값
스토리지 노드 A NFS LIF 01 IP입니다	<<var_NodeA_nfs_lif_01_ip>>
스토리지 노드 A NFS LIF 01 네트워크 마스크	<<var_NodeA_nfs_lif_01_mask>>
스토리지 노드 B NFS LIF 02 IP	<<var_NodeB_nfs_lif_02_ip>>
스토리지 노드 B NFS LIF 02 네트워크 마스크	<<var_NodeB_nfs_lif_02_mask>>

1. NFS LIF를 생성합니다.

```
network interface create -vserver Infra-SVM -lif nfs_lif01 -role data
-data-protocol nfs -home-node <<var_nodeA>> -home-port a0a-
<<var_nfs_vlan_id>> -address <<var_nodeA_nfs_lif_01_ip>> -netmask <<
var_nodeA_nfs_lif_01_mask>> -status-admin up -failover-policy broadcast-
domain-wide -firewall-policy data -auto-revert true
network interface create -vserver Infra-SVM -lif nfs_lif02 -role data
-data-protocol nfs -home-node <<var_nodeA>> -home-port a0a-
<<var_nfs_vlan_id>> -address <<var_nodeB_nfs_lif_02_ip>> -netmask <<
var_nodeB_nfs_lif_02_mask>> -status-admin up -failover-policy broadcast-
domain-wide -firewall-policy data -auto-revert true
network interface show
```

인프라 **SVM** 관리자를 추가합니다

다음 표에는 이 구성을 완료하는 데 필요한 정보가 나와 있습니다.

세부 정보	상세 값
Vsmgmt IP	<<var_svm_mgmt_ip>> 를 입력합니다
Vsmgmt 네트워크 마스크	<<var_svm_mgmt_mask>>
Vsmgmt 기본 게이트웨이	<<var_svm_mgmt_gateway>>

관리 네트워크에 인프라 SVM 관리자 및 SVM 관리 논리 인터페이스를 추가하려면 다음 단계를 완료하십시오.

1. 다음 명령을 실행합니다.

```
network interface create -vserver Infra-SVM -lif vsmgmt -role data
-data-protocol none -home-node <<var_nodeB>> -home-port  e0M -address
<<var_svm_mgmt_ip>> -netmask <<var_svm_mgmt_mask>> -status-admin up
-failover-policy broadcast-domain-wide -firewall-policy mgmt -auto-
revert true
```

ⓘ 여기서 SVM 관리 IP는 스토리지 클러스터 관리 IP와 동일한 서브넷에 있어야 합니다.

2. 기본 경로를 생성하여 SVM 관리 인터페이스가 외부 환경에 도달할 수 있도록 합니다.

```
network route create -vserver Infra-SVM -destination 0.0.0.0/0 -gateway
<<var_svm_mgmt_gateway>>
network route show
```

3. SVM vsadmin 사용자의 암호를 설정하고 사용자 잠금을 해제합니다.

```
security login password -username vsadmin -vserver Infra-SVM
Enter a new password: <<var_password>>
Enter it again: <<var_password>>
security login unlock -username vsadmin -vserver Infra-SVM
```

"다음: Cisco UCS C-Series 랙 서버 구현 절차"

Cisco UCS C-Series 랙 서버 구축 절차

다음 섹션에서는 FlexPod Express 구성에 사용할 Cisco UCS C-Series 독립 실행형 랙 서버를 구성하기 위한 절차를 세부적으로 설명합니다.

Cisco 통합 관리 서버에 대한 초기 **Cisco UCS C-Series** 독립 실행형 서버 설정을 수행합니다

Cisco UCS C-Series 독립 실행형 서버에 대한 CIMC 인터페이스의 초기 설정을 위해 다음 단계를 완료합니다.

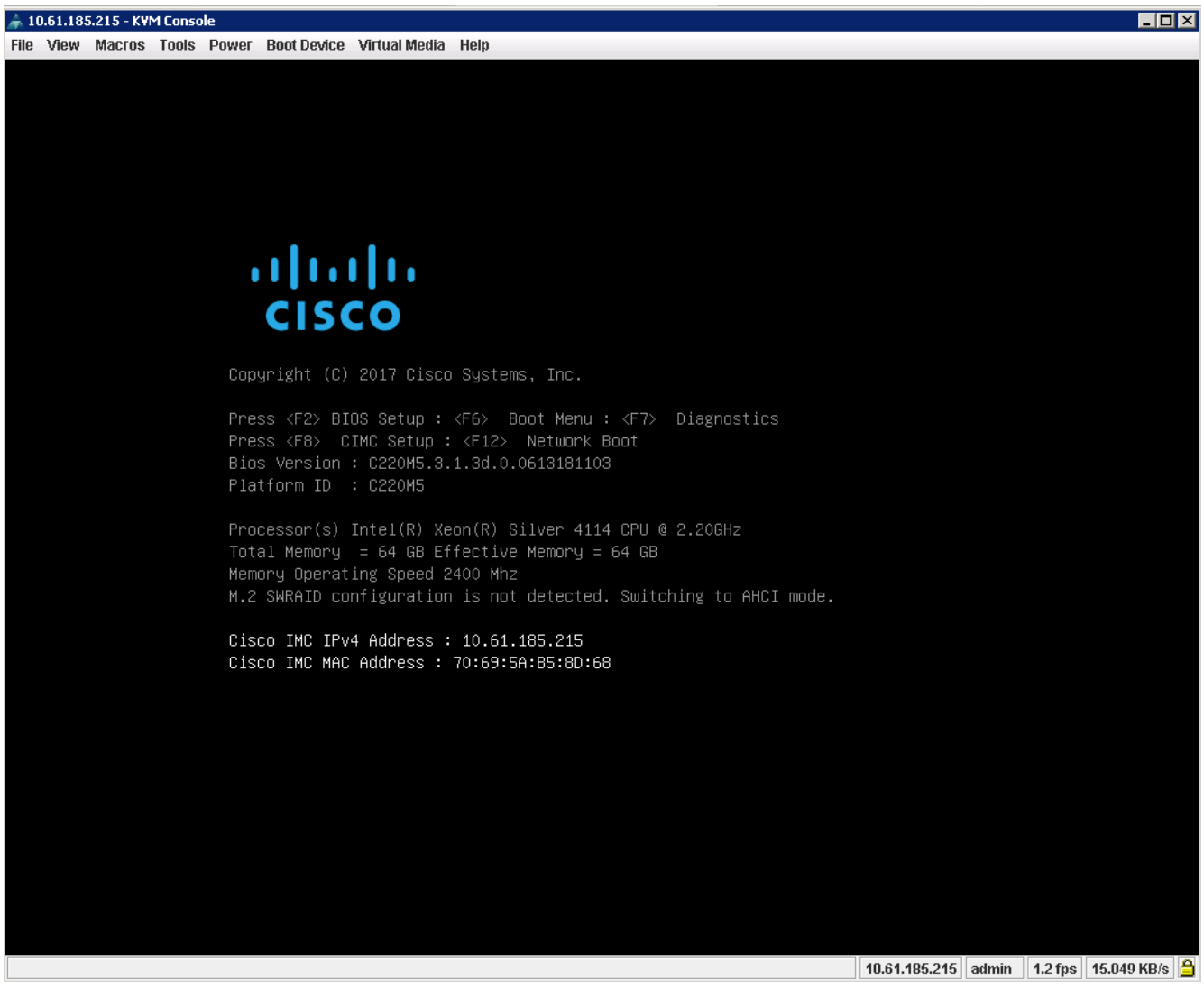
다음 표에는 각 Cisco UCS C-Series 독립 실행형 서버에 대한 CIMC를 구성하는 데 필요한 정보가 나와 있습니다.

세부 정보	상세 값
CIMC IP 주소	CIMC_IP>\< CIMC_IP>>
CIMC 서브넷 마스크	CIMC_Netmask>\<CIMC_NETMASK>>
CIMC 기본 게이트웨이	CIMC_GATELOGATE>\<<CIMC_Gateway>

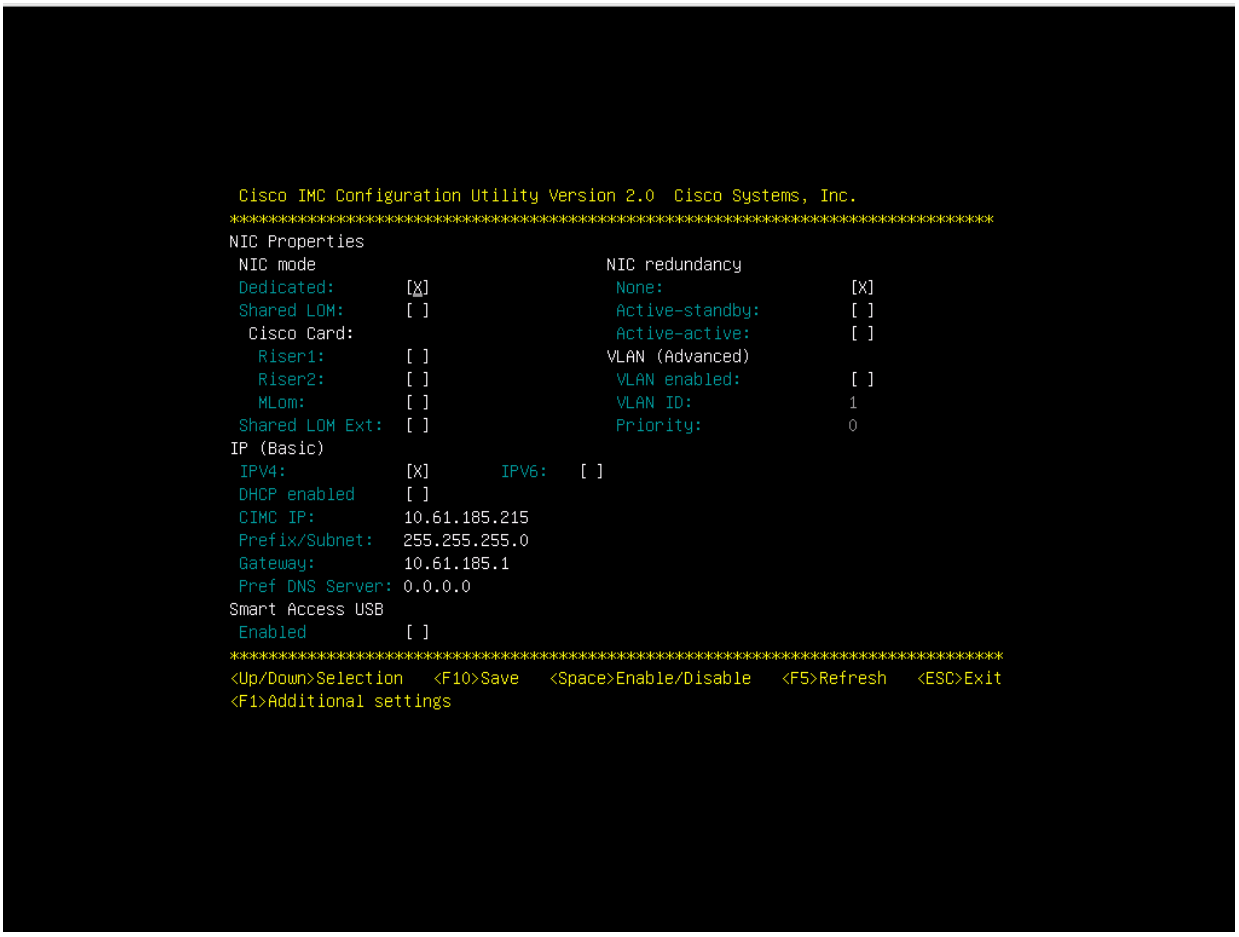
이 검증에 사용된 CIMC 버전은 CIMC 3.1.3(g)입니다.

모든 서버

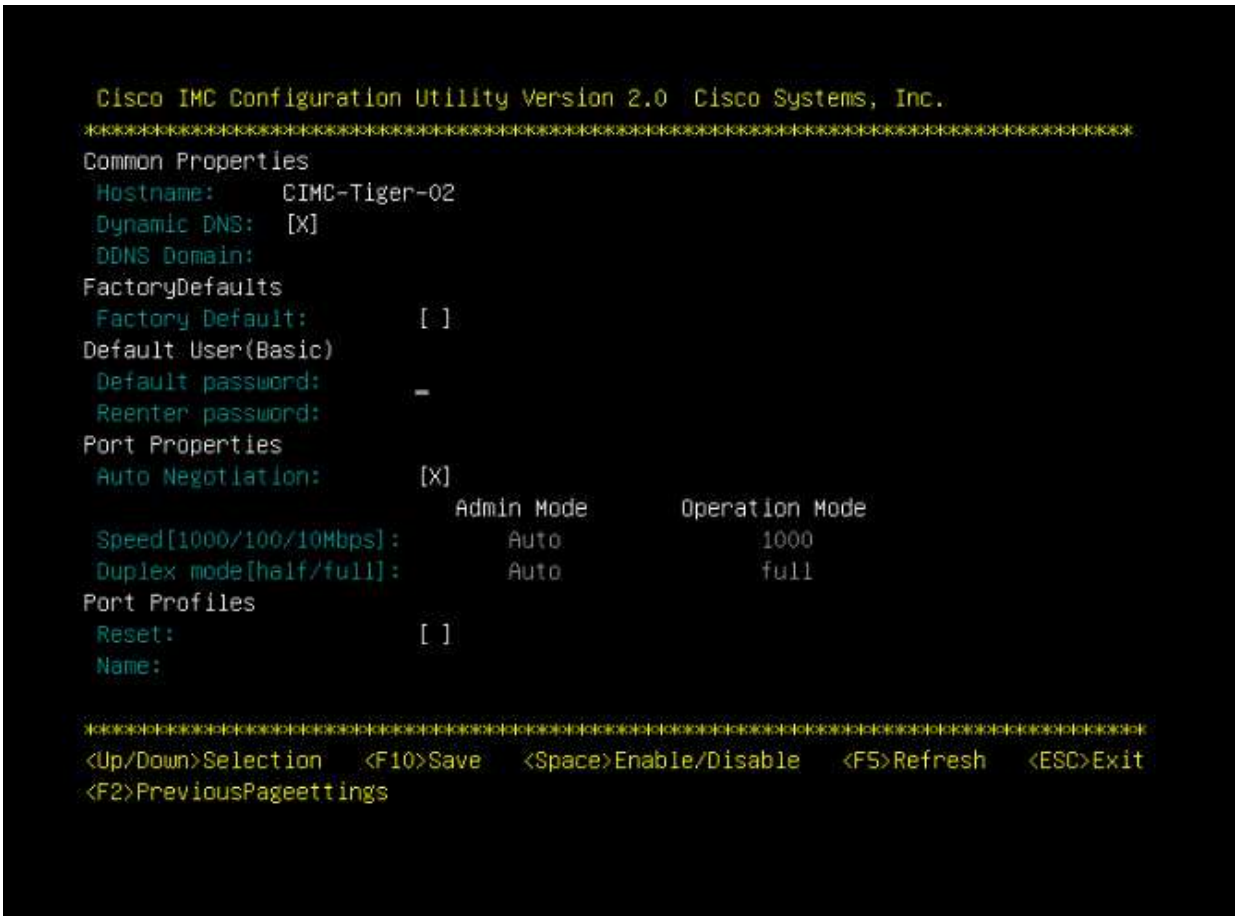
1. 서버와 함께 제공된 Cisco 키보드, 비디오 및 마우스(KVM) 동글을 서버 앞의 KVM 포트에 연결합니다. VGA 모니터와 USB 키보드의 플러그를 적절한 KVM 동글 포트에 꽂습니다.
2. 서버의 전원을 켜고 CIMC 구성을 시작할지 묻는 메시지가 표시되면 F8 키를 누릅니다.



3. CIMC 구성 유틸리티에서 다음 옵션을 설정합니다.
   - 네트워크 인터페이스 카드(NIC) 모드:
     - 전용 [X]
   - IP(기본):
     - IPv4: [X]
     - DHCP 활성화: [ ]
     - CIMC IP:<<CIMC_IP>>
     - 접두사/서브넷:\< CIMC_Netmask>>
     - 게이트웨이:<<CIMC_Gateway>>
   - VLAN(고급): VLAN 태깅을 사용하지 않도록 설정하려면 선택되지 않은 상태로 둡니다.
     - NIC 이중화
     - 없음: [X]



4. 추가 설정을 보려면 F1 키를 누릅니다.
   - 공통 속성:
     - 호스트 이름:\< ESXi_host_name>>
     - 동적 DNS: [ ]
     - 공장 출하시 기본값: 선택하지 않은 상태로 둡니다.
   - 기본 사용자(기본):
     - 기본 암호:<<admin_password>>
     - 암호 <<admin_password>>를 다시 입력하십시오
     - 포트 속성: 기본값을 사용합니다.
     - 포트 프로파일: 선택하지 않은 상태로 둡니다.



5. F10 키를 눌러 CIMC 인터페이스 구성을 저장합니다.
6. 구성을 저장한 후 Esc 키를 눌러 종료합니다.

Cisco UCS C-Series 서버 iSCSI 부팅을 구성합니다

이 FlexPod Express 구성에서 VIC1387은 iSCSI 부팅에 사용됩니다.

다음 표에는 iSCSI 부트를 구성하는 데 필요한 정보가 나와 있습니다.

기울임꼴로 표시된 글꼴은 각 ESXi 호스트에 대해 고유한 변수를 나타냅니다.

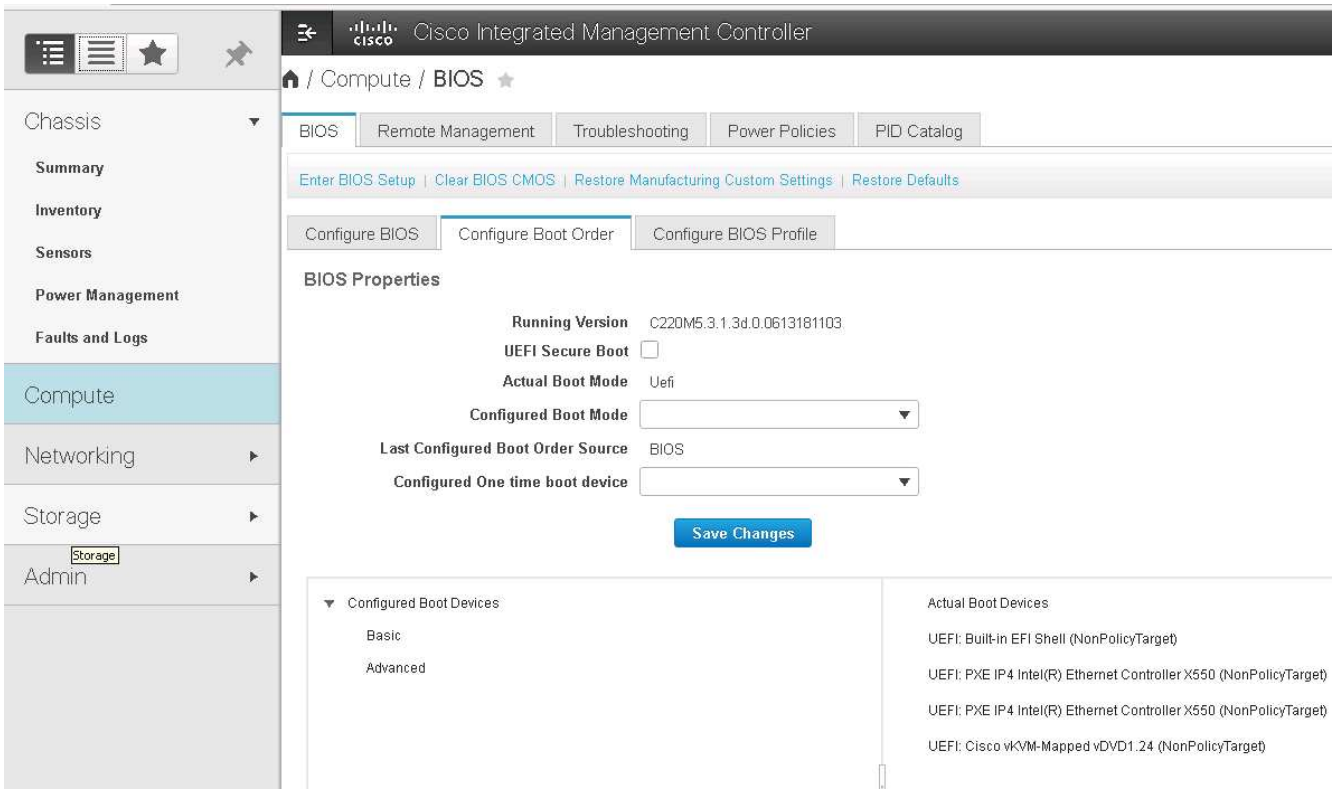
세부 정보	상세 값
ESXi 호스트 이니시에이터에서 이름을 입력합니다	<<var_UCS_initiator_name_a>>
ESXi 호스트 iSCSI - A IP	<<var_esxi_host_iscsiA_ip>>
ESXi 호스트 iSCSI - 네트워크 마스크입니다	<<var_esxi_host_iscsiA_mask>>
ESXi 호스트 iSCSI 기본 게이트웨이입니다	<<var_esxi_host_iscsiA_gateway>>
ESXi 호스트 이니시에이터 B 이름입니다	<<var_UCS_initiator_name_B>>
ESXi 호스트 iSCSI-B IP	<<var_esxi_host_iscsiB_ip>>
ESXi 호스트 iSCSI-B 네트워크 마스크	<<var_esxi_host_iscsiB_mask>>
ESXi 호스트 iSCSI-B 게이트웨이	<<var_esxi_host_iscsiB_gateway>>

세부 정보	상세 값
IP 주소 iscsi_liff 01a	
IP 주소 iscsi_lif02a	
IP 주소 iscsi_liff 01b	
IP 주소 iscsi_liff 02b	
infra_SVM IQN을 선택합니다	

부팅 순서 구성

부팅 순서 구성을 설정하려면 다음 단계를 수행하십시오.

1. CIMC 인터페이스 브라우저 창에서 Server 탭을 클릭하고 BIOS를 선택합니다.
2. Configure Boot Order(부팅 순서 구성) 를 클릭한 다음 OK(확인) 를 클릭합니다.



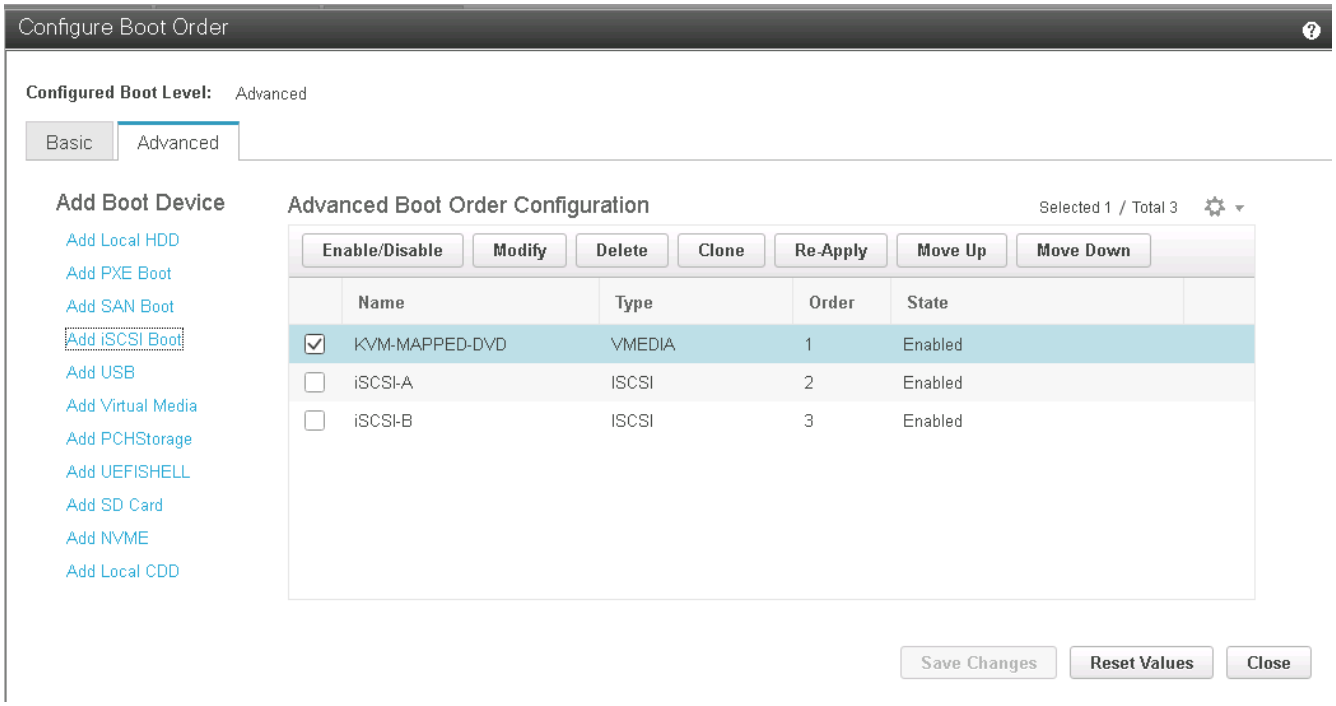
3. Add Boot Device(부팅 장치 추가) 에서 장치를 클릭하고 Advanced(고급) 탭으로 이동하여 다음 장치를 구성합니다.
   - 가상 미디어를 추가합니다
     - 이름: kvm-cd-dvd
     - 하위 유형: KVM 매핑된 DVD
     - 상태: 활성화됨
     - 순서: 1
   - iSCSI 부트를 추가합니다.

- 이름: iscsi-a
- 상태: 활성화됨
- 주문: 2
- 슬롯: mLOM
- 포트: 0

◦ Add iSCSI Boot 를 클릭합니다.

- 이름: iSCSI-B
- 상태: 활성화됨
- 순서: 3
- 슬롯: mLOM
- 포트: 1

4. 장치 추가를 클릭합니다.
5. 변경 내용 저장 을 클릭한 다음 닫기 를 클릭합니다.



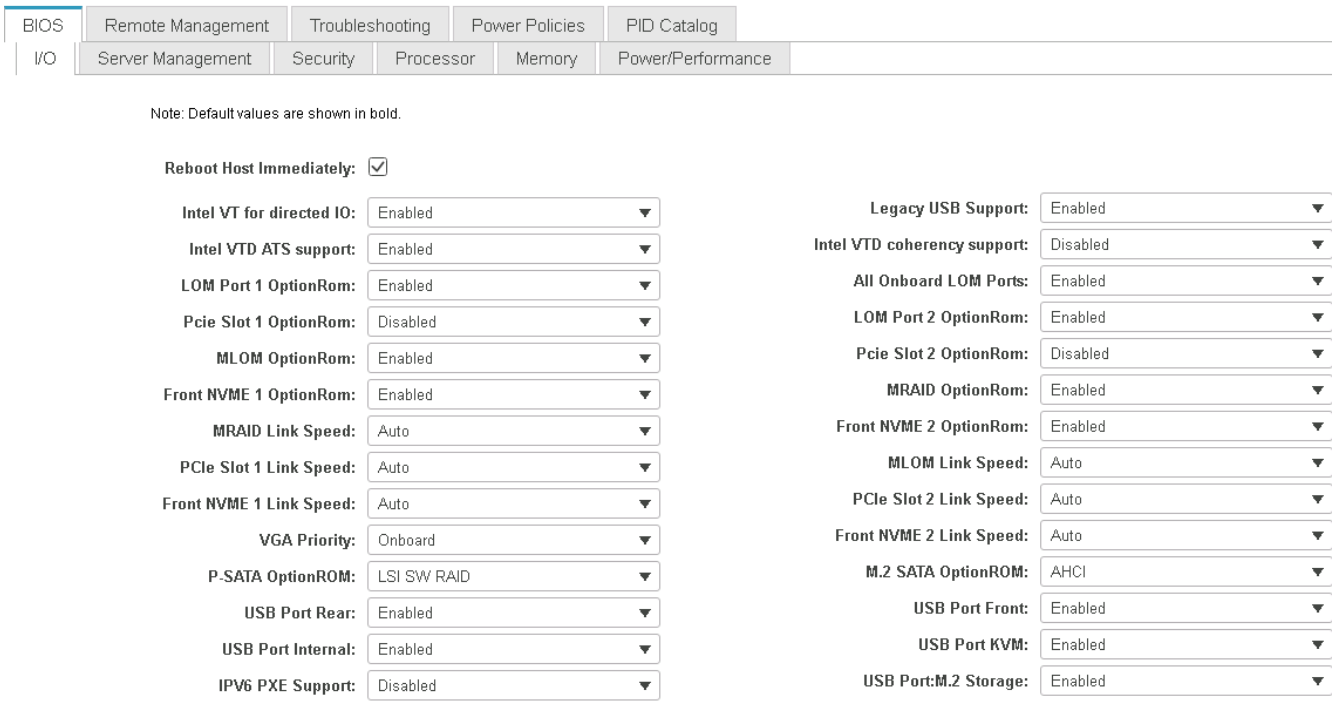
6. 새 부팅 순서로 부팅하려면 서버를 재부팅합니다.

RAID 컨트롤러 비활성화(있는 경우)

C 시리즈 서버에 RAID 컨트롤러가 포함되어 있는 경우 다음 단계를 수행하십시오. SAN 구성으로 부팅할 때 RAID 컨트롤러가 필요하지 않습니다. 선택적으로 서버에서 RAID 컨트롤러를 물리적으로 제거할 수도 있습니다.

1. CIMC의 왼쪽 탐색 창에서 BIOS를 클릭합니다.
2. Configure BIOS 를 선택합니다.
3. PCIe 슬롯: HBA 옵션 ROM으로 아래로 스크롤합니다.

4. 이 값이 아직 비활성화되지 않은 경우 비활성화로 설정합니다.



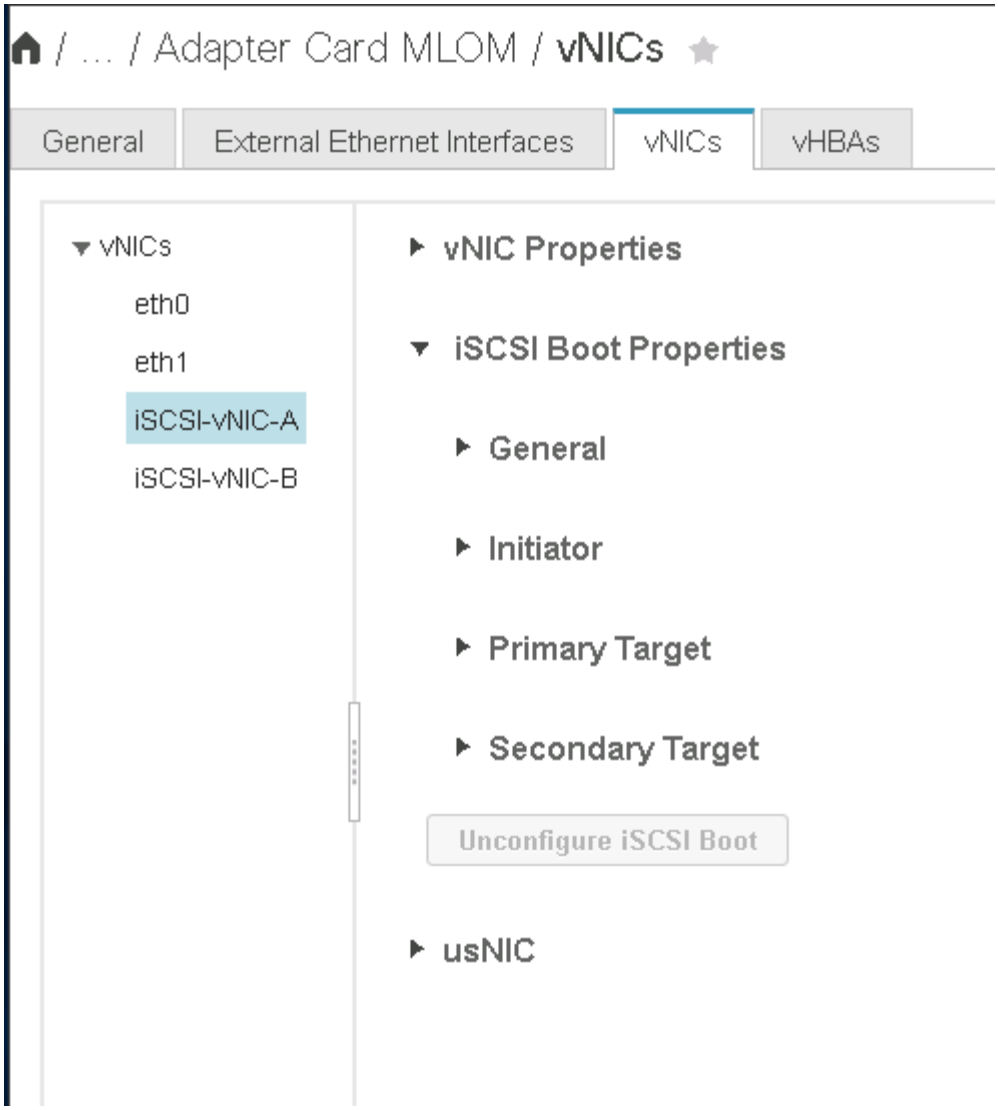
iSCSI 부트에 대해 **Cisco VIC1387**을 구성합니다

다음 구성 단계는 iSCSI 부트에 대한 Cisco VIC 1387에 대한 것입니다.

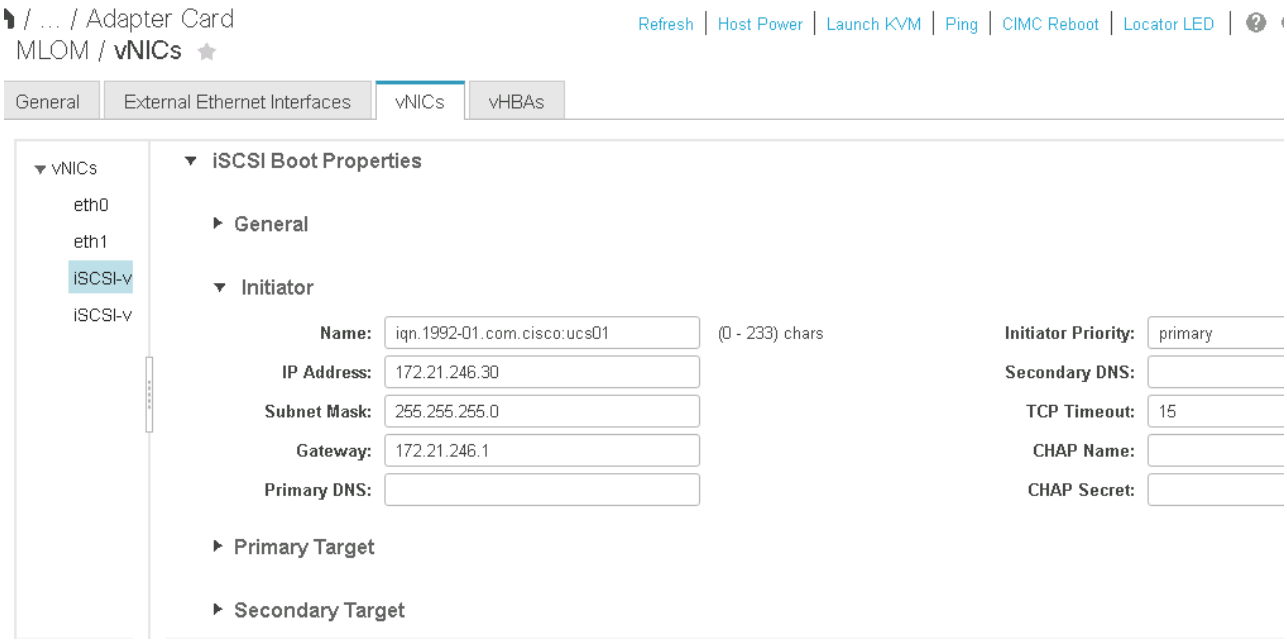
iSCSI vNIC를 생성합니다

1. 추가 를 클릭하여 vNIC를 생성합니다.
2. vNIC 추가 섹션에서 다음 설정을 입력합니다.
   - 이름: iscsi-vNIC-A
   - MTU: 9000
   - 기본 VLAN:<<var_iscsi_vlan_a>>'입니다
   - VLAN 모드: 트렁크
   - PXE 부팅 활성화: 확인

3. vNIC 추가 를 클릭한 다음 확인 을 클릭합니다.
4. 이 과정을 반복하여 두 번째 vNIC를 추가합니다.
   a. vNIC의 이름을 iSCSI-vNIC-B로 지정합니다.
   b. VLAN으로 '<<var_iscsi_vlan_b>>'를 입력합니다.
   c. 업링크 포트를 "1"로 설정합니다.
5. 왼쪽에서 vNIC의 iSCSI-vNIC-A를 선택합니다.



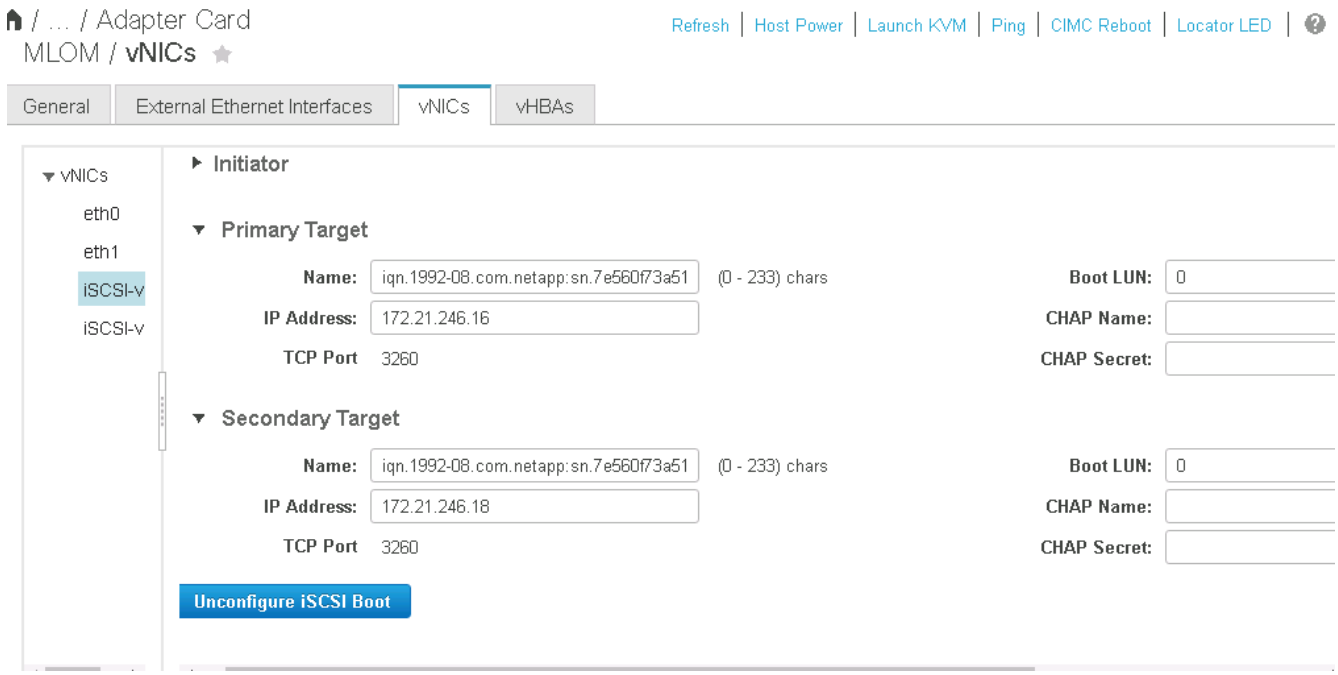
6. iSCSI 부트 속성에서 이니시에이터 세부 정보를 입력합니다.
   - 이름:<<var_ucsa_initiator_name_a>>
   - IP 주소:<<var_esxi_hostA_iscsiA_ip>>
   - 서브넷 마스크:<<var_esxi_hostA_iscsiA_mask>>
   - 게이트웨이:<<var_esxi_hostA_iscsiA_gateway>>



7. 기본 타겟 세부 정보를 입력합니다.
   - 이름: 인프라 SVM의 IQN 번호입니다
   - IP 주소: iSCSI_liff 01a IP 주소
   - 부팅 LUN: 0
8. 2차 타겟 세부 정보를 입력합니다.
   - 이름: 인프라 SVM의 IQN 번호입니다
   - IP address: iSCSI_liff 02a의 IP 주소입니다
   - 부팅 LUN: 0

   "vserver iscsi show" 명령을 실행하여 스토리지 IQN 번호를 확인할 수 있습니다.

   각 vNIC의 IQN 이름을 기록해야 합니다. 나중에 필요한 단계일 수 있습니다.



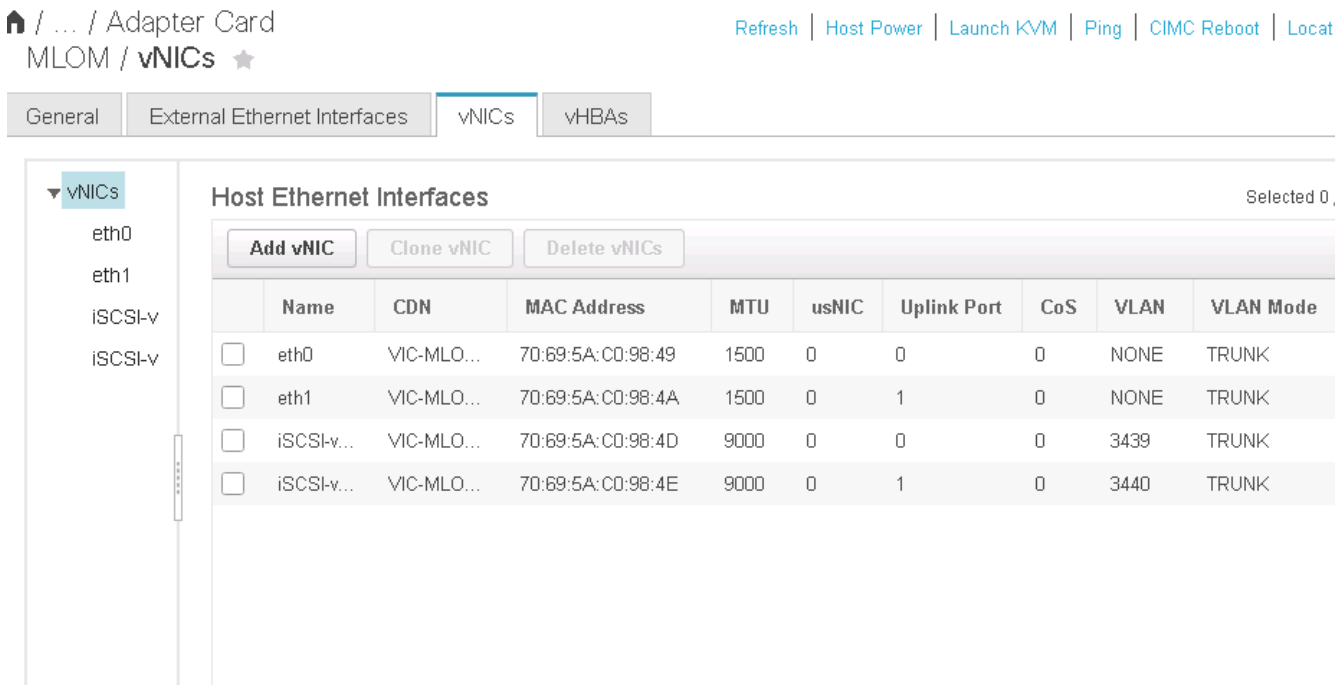
9. Configure iSCSI 를 클릭합니다.
10. vNIC의 iSCSI-vNIC-B를 선택하고 Host Ethernet Interfaces 섹션 상단에 있는 iSCSI Boot 버튼을 클릭합니다.
11. 이 과정을 반복하여 iSCSI-vNIC-B를 구성합니다.
12. 이니시에이터 세부 정보를 입력합니다.
    - 이름:<<var_ucsa_initiator_name_b>>'
    - IP 주소: "<<var_esxi_hostB_iscsib_ip>>"
    - 서브넷 마스크: "<<var_esxi_hostB_iscsib_mask>>"
    - 게이트웨이:\<<var_esxi_hostB_iscsib_gateway>'
13. 기본 타겟 세부 정보를 입력합니다.
    - 이름: 인프라 SVM의 IQN 번호입니다
    - IP 주소: iSCSI_liff 01b 의 IP 주소입니다
    - 부팅 LUN: 0
14. 2차 타겟 세부 정보를 입력합니다.
    - 이름: 인프라 SVM의 IQN 번호입니다
    - IP 주소: iSCSI_liff 02b의 IP 주소입니다
    - 부팅 LUN: 0

    "vserver iscsi show" 명령을 사용하여 스토리지 IQN 번호를 가져올 수 있습니다.

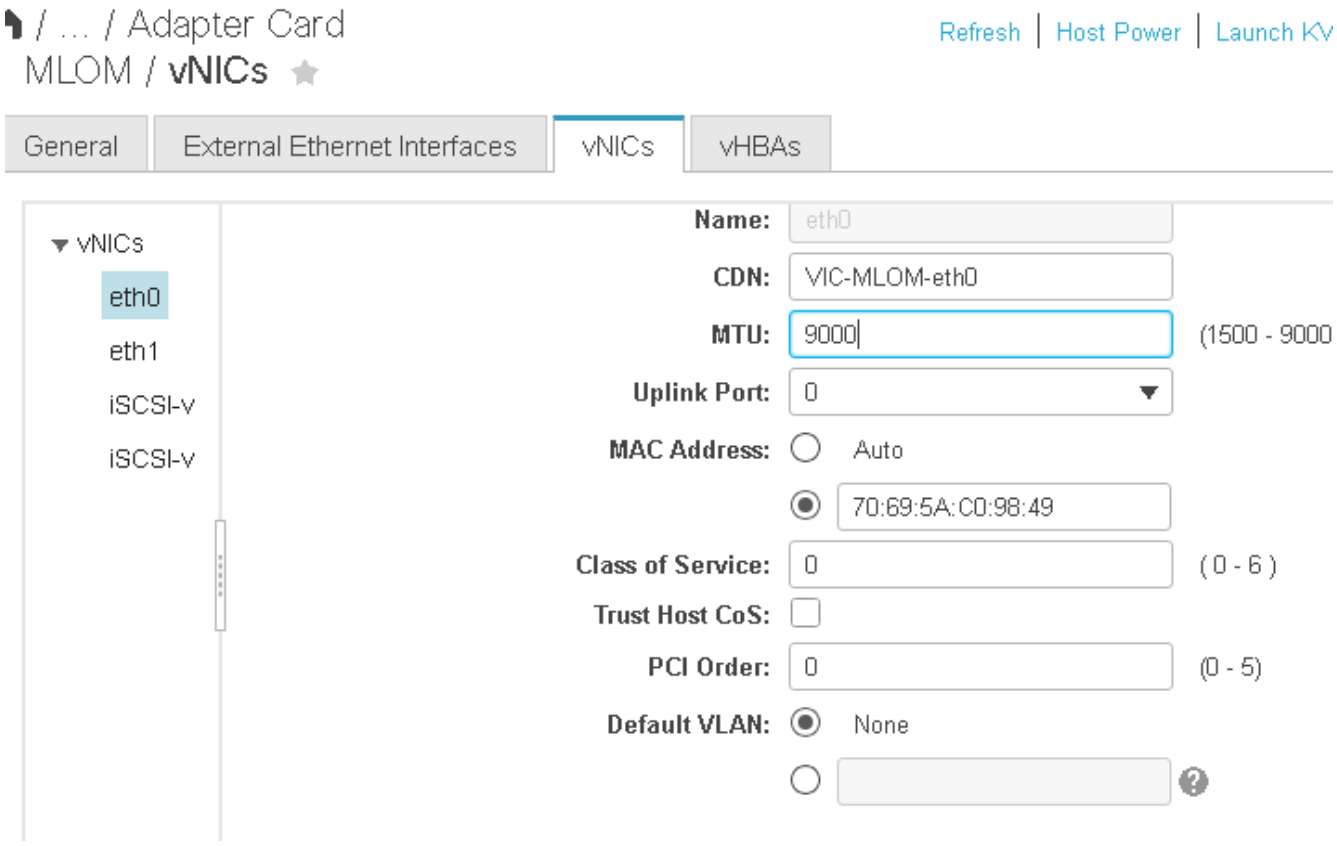
    각 vNIC의 IQN 이름을 기록해야 합니다. 나중에 필요한 단계일 수 있습니다.
15. Configure iSCSI 를 클릭합니다.
16. 이 프로세스를 반복하여 Cisco UCS 서버 B에 대한 iSCSI 부팅을 구성합니다

ESXi용 vNIC를 구성합니다

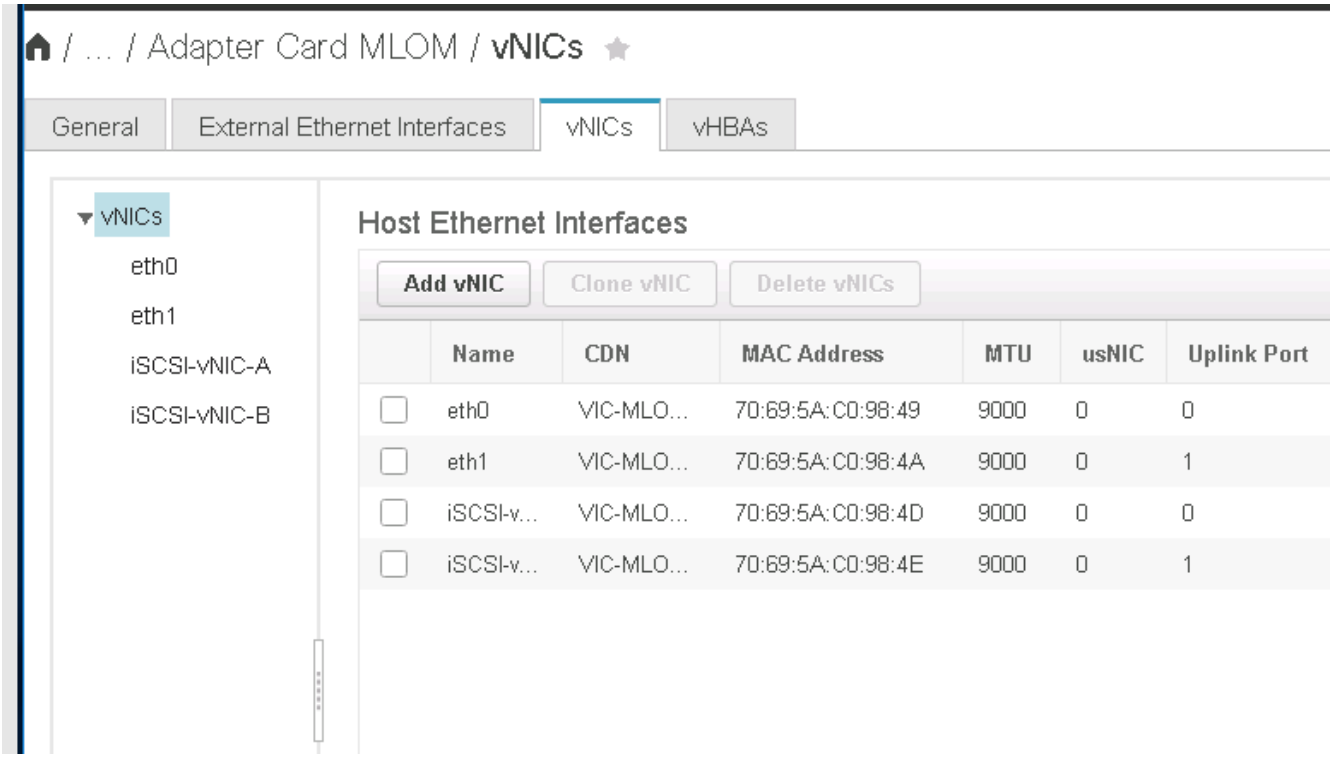
1. CIMC 인터페이스 브라우저 창에서 인벤토리 를 클릭한 다음 오른쪽 창에서 Cisco VIC 어댑터 를 클릭합니다.
2. 어댑터 카드 아래에서 Cisco UCS VIC 1387을 선택한 다음 아래에서 vNIC를 선택합니다.



3. eth0 을 선택하고 속성 을 클릭합니다.
4. MTU를 9000으로 설정합니다. 변경 내용 저장 을 클릭합니다.



5. eth1에 대해 3단계와 4단계를 반복하여 업링크 포트가 eth1에 대해 "1"로 설정되어 있는지 확인합니다.



이 절차는 각 초기 Cisco UCS 서버 노드 및 환경에 추가된 각 추가 Cisco UCS 서버 노드에 대해 반복해야 합니다.

"다음: NetApp AFF 스토리지 구현 절차(2부)"

NetApp AFF 스토리지 구현 절차(2부)

ONTAP SAN 부팅 스토리지 설정

iSCSI igroup을 생성합니다

Igroup을 생성하려면 다음 단계를 완료하십시오.

이 단계를 위해서는 서버 구성에서 iSCSI 이니시에이터 IQN이 필요합니다.

1. 클러스터 관리 노드의 SSH 연결에서 다음 명령을 실행합니다. 이 단계에서 생성한 3개의 igroup을 보려면 igroup show 명령을 실행합니다.

```
igroup create –vserver Infra-SVM –igroup VM-Host-Infra-A –protocol iscsi
–ostype vmware –initiator <<var_vm_host_infra_a_iSCSI-A_vNIC_IQN>>,
<<var_vm_host_infra_a_iSCSI-B_vNIC_IQN>>
igroup create –vserver Infra-SVM –igroup VM-Host-Infra-B –protocol iscsi
–ostype vmware –initiator <<var_vm_host_infra_b_iSCSI-A_vNIC_IQN>>,
<<var_vm_host_infra_b_iSCSI-B_vNIC_IQN>>
```

ⓘ Cisco UCS C-Series 서버를 추가할 때는 이 단계를 완료해야 합니다.

부팅 LUN을 igroup에 매핑합니다

부트 LUN을 igroup에 매핑하려면 클러스터 관리 SSH 연결에서 다음 명령을 실행합니다.

```
lun map –vserver Infra-SVM –volume esxi_boot –lun VM-Host-Infra- A –igroup
VM-Host-Infra- A –lun-id 0
lun map –vserver Infra-SVM –volume esxi_boot –lun VM-Host-Infra- B –igroup
VM-Host-Infra- B –lun-id 0
```

ⓘ Cisco UCS C-Series 서버를 추가할 때는 이 단계를 완료해야 합니다.

"다음: VMware vSphere 6.7 구축 절차."

VMware vSphere 6.7 구축 절차

이 섹션에서는 FlexPod Express 구성에 VMware ESXi 6.7을 설치하는 절차를 자세히 설명합니다. 다음 구현 절차는 이전 섹션에서 설명한 환경 변수를 포함하도록 커스터마이징되었습니다.

이러한 환경에 VMware ESXi를 설치하는 방법은 여러 가지가 있습니다. 이 절차에서는 Cisco UCS C-Series 서버용 CIMC 인터페이스의 가상 KVM 콘솔과 가상 미디어 기능을 사용하여 원격 설치 미디어를 각 개별 서버에 매핑합니다.

이 절차는 Cisco UCS 서버 A 및 Cisco UCS 서버 B에 대해 완료되어야 합니다

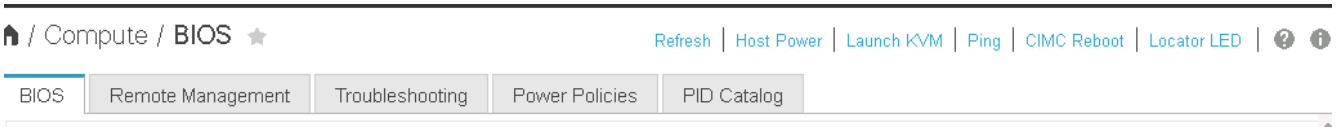
클러스터에 추가된 노드에 대해 이 절차를 완료해야 합니다.

Cisco UCS C-Series 독립 실행형 서버에 대한 CIMC 인터페이스에 로그인합니다

다음 단계에서는 Cisco UCS C-Series 독립 실행형 서버의 CIMC 인터페이스에 로그인하는 방법을 자세히 설명합니다. CIMC 인터페이스에 로그인하여 가상 KVM을 실행해야 관리자가 원격 미디어를 통해 운영 체제 설치를 시작할 수 있습니다.

모든 호스트

1. 웹 브라우저로 이동하고 Cisco UCS C-Series의 CIMC 인터페이스에 대한 IP 주소를 입력합니다. 이 단계에서는 CIMC GUI 애플리케이션이 시작됩니다.
2. 관리자의 사용자 이름과 자격 증명을 사용하여 CIMC UI에 로그인합니다.
3. 주 메뉴에서 서버 탭을 선택합니다.
4. Launch KVM Console을 클릭합니다.



5. 가상 KVM 콘솔에서 Virtual Media 탭을 선택합니다.
6. CD/DVD 매핑 을 선택합니다.

먼저 가상 디바이스 활성화 를 클릭해야 할 수도 있습니다. 메시지가 표시되면 이 세션 수락 을 선택합니다.

7. VMware ESXi 6.7 설치 관리자 ISO 이미지 파일을 찾아 이동하고 Open을 클릭합니다. 장치 매핑 을 클릭합니다.
8. Power 메뉴를 선택하고 Power Cycle System (Cold Boot) 을 선택합니다. 예 를 클릭합니다.

VMware ESXi를 설치합니다

다음 단계에서는 각 호스트에 VMware ESXi를 설치하는 방법을 설명합니다.

ESXi 6.7 Cisco 사용자 지정 이미지를 다운로드합니다

1. 로 이동합니다 "VMware vSphere 다운로드 페이지" 사용자 정의 ISO의 경우.
2. Cisco Custom Image for ESXi 6.7 GA Install CD(ESXi 6.7 GA 설치 CD용 Cisco 사용자 지정 이미지) 옆의 Go to Downloads(다운로드로 이동) 를 클릭합니다.
3. ESXi 6.7 GA 설치 CD(ISO)용 Cisco Custom Image를 다운로드합니다.

모든 호스트

1. 시스템이 부팅되면 VMware ESXi 설치 미디어의 존재 여부가 자동으로 감지됩니다.
2. 나타나는 메뉴에서 VMware ESXi 설치 프로그램을 선택합니다.

설치 프로그램이 로드됩니다. 이 작업은 몇 분 정도 걸립니다.

3. 설치 프로그램 로드가 완료된 후 Enter 키를 눌러 설치를 계속합니다.
4. 최종 사용자 사용권 계약을 읽은 후 동의하고 F11 키를 눌러 설치를 계속합니다.
5. 이전에 ESXi용 설치 디스크로 설정된 NetApp LUN을 선택하고 Enter 키를 눌러 설치를 계속합니다.

6. 적절한 자판 배열을 선택하고 Enter 키를 누릅니다.
7. 루트 암호를 입력 및 확인하고 Enter 키를 누릅니다.
8. 볼륨에서 기존 파티션이 제거된다는 경고 메시지가 표시됩니다. F11 키를 눌러 설치를 계속합니다. ESXi 설치 후 서버가 재부팅됩니다.

VMware ESXi 호스트 관리 네트워킹을 설정합니다

다음 단계에서는 각 VMware ESXi 호스트의 관리 네트워크를 추가하는 방법을 설명합니다.

모든 호스트

1. 서버 재부팅이 완료된 후 F2 키를 눌러 시스템 커스터마이징 옵션을 시작합니다.
2. root라는 로그인 이름과 이전에 설치 과정에서 입력한 루트 암호를 사용하여 로그인합니다.
3. Configure Management Network 옵션을 선택합니다.
4. Network Adapters 를 선택하고 Enter 키를 누릅니다.
5. vSwitch0에 대해 원하는 포트를 선택합니다. Enter 키를 누릅니다.

CIMC의 eth0 및 eth1에 해당하는 포트를 선택합니다.

6. VLAN (optional)을 선택하고 Enter 키를 누릅니다.
7. VLAN ID '<<mgmt_vlan_id>>'를 입력합니다. Enter 키를 누릅니다.
8. Configure Management Network 메뉴에서 IPv4 Configuration을 선택하여 관리 인터페이스의 IP 주소를 구성합니다. Enter 키를 누릅니다.
9. 화살표 키를 사용하여 Set Static IPv4 address(정적 IPv4 주소 설정) 를 강조 표시하고 스페이스바를 사용하여 이 옵션을 선택합니다.
10. VMware ESXi 호스트 "\< ESXi_host_mgmt_ip>>"를 관리하기 위한 IP 주소를 입력합니다.
11. VMware ESXi 호스트 "\< ESXi_host_mgmt_netmask>>의 서브넷 마스크를 입력합니다
12. VMware ESXi 호스트 '\< ESXi_host_mgmt_gateway>'의 기본 게이트웨이를 입력합니다.
13. Enter 키를 눌러 IP 구성의 변경 사항을 적용합니다.
14. IPv6 구성 메뉴로 들어갑니다.
15. 스페이스바를 사용하여 IPv6 사용(재시작 필요) 옵션을 선택 취소하여 IPv6을 사용하지 않도록 설정합니다. Enter 키를 누릅니다.
16. DNS 설정을 구성하는 메뉴로 들어갑니다.
17. IP 주소는 수동으로 할당되므로 DNS 정보도 수동으로 입력해야 합니다.
18. Primary DNS 서버의 IP 주소를 입력합니다[nameserver_ip]".
19. (선택 사항) 보조 DNS 서버의 IP 주소를 입력합니다.
20. VMware ESXi 호스트 이름:'에 대한 FQDN을 입력합니다[esxi_host_fqdn]".
21. Enter 키를 눌러 DNS 구성의 변경 사항을 적용합니다.
22. Esc 키를 눌러 Configure Management Network 하위 메뉴를 종료합니다.
23. Y 를 눌러 변경 사항을 확인하고 서버를 재부팅합니다.
24. Esc 키를 눌러 VMware 콘솔에서 로그아웃합니다.

ESXi 호스트를 구성합니다

각 ESXi 호스트를 구성하려면 다음 표의 정보가 필요합니다.

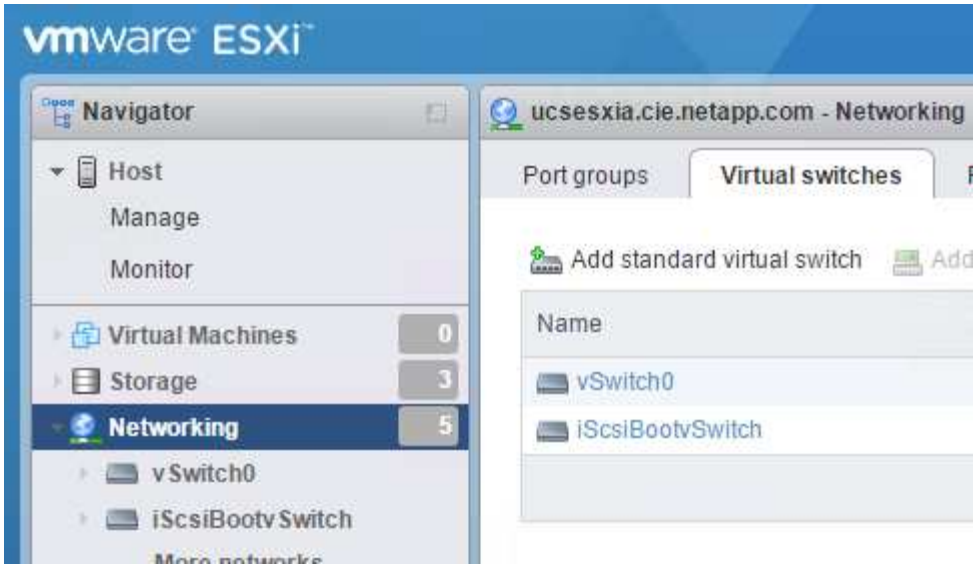
세부 정보	값
ESXi 호스트 이름입니다	
ESXi 호스트 관리 IP입니다	
ESXi 호스트 관리 마스크입니다	
ESXi 호스트 관리 게이트웨이	
ESXi 호스트 NFS IP입니다	
ESXi 호스트 NFS 마스크입니다	
ESXi 호스트 NFS 게이트웨이	
ESXi 호스트 vMotion IP입니다	
ESXi 호스트 vMotion 마스크	
ESXi 호스트 vMotion 게이트웨이	
ESXi 호스트 iSCSI - A IP	
ESXi 호스트 iSCSI - 마스크	
ESXi 호스트 iSCSI - 게이트웨이	
ESXi 호스트 iSCSI-B IP	
ESXi 호스트 iSCSI-B 마스크	
ESXi 호스트 iSCSI-B 게이트웨이	

ESXi 호스트에 로그인합니다

1. 웹 브라우저에서 호스트의 관리 IP 주소를 엽니다.
2. 설치 프로세스 중에 지정한 암호 및 루트 계정을 사용하여 ESXi 호스트에 로그인합니다.
3. VMware 사용자 환경 개선 프로그램에 대한 설명을 읽어 보십시오. 적절한 응답을 선택한 후 OK(확인) 를 클릭합니다.

iSCSI 부트를 구성합니다

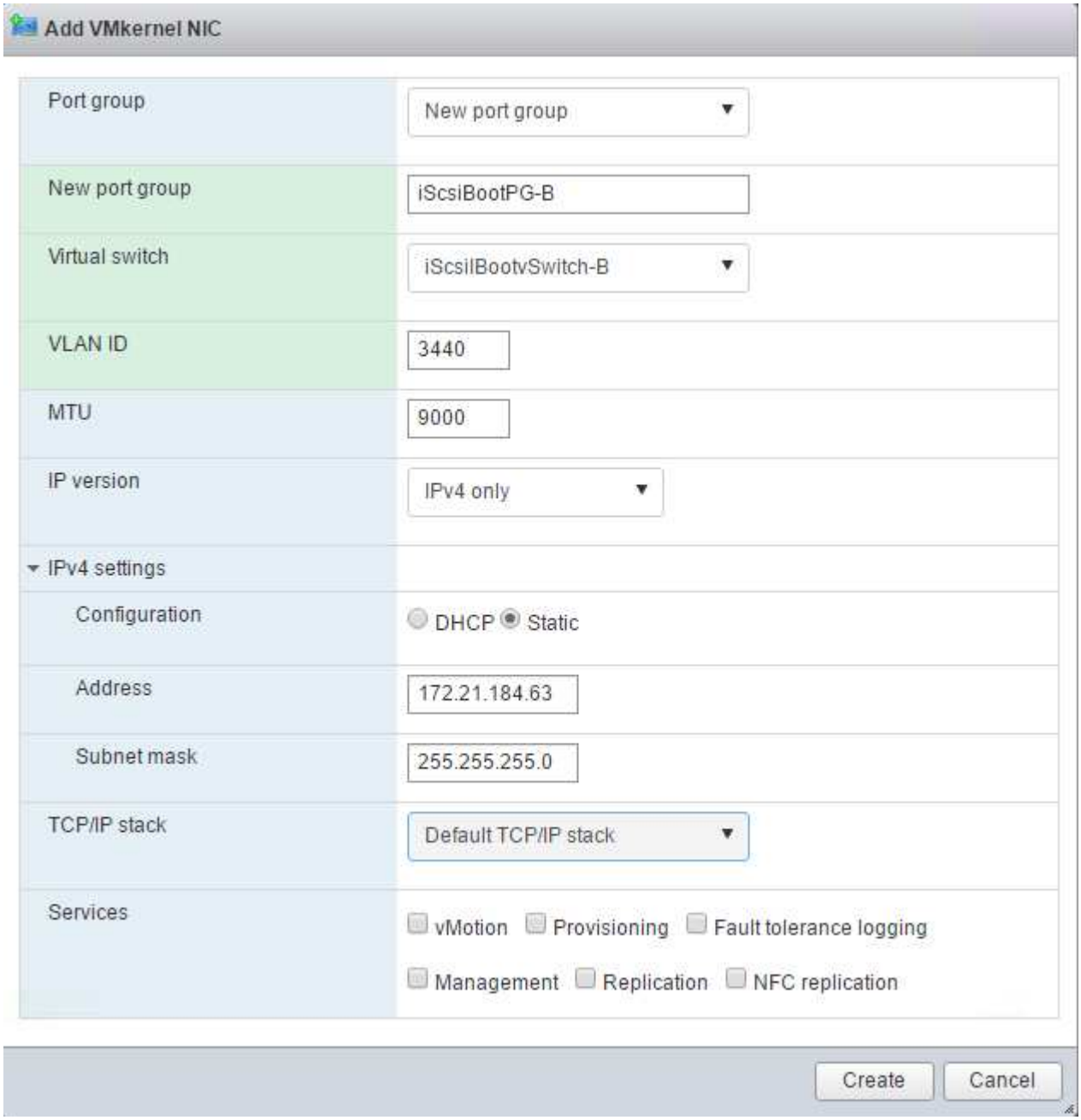
1. 왼쪽에서 네트워킹 을 선택합니다.
2. 오른쪽에서 Virtual Switches 탭을 선택합니다.



3. iSciBootvSwitch 를 클릭합니다.
4. 설정 편집 을 선택합니다.
5. MTU를 9000으로 변경하고 저장 을 클릭합니다.
6. 가상 스위치 탭으로 돌아가려면 왼쪽 탐색 창에서 네트워킹 을 클릭합니다.
7. 표준 가상 스위치 추가를 클릭합니다.
8. vSwitch 이름에 iSciBootvSwitch-B라는 이름을 입력합니다.
   - MTU를 9000으로 설정합니다.
   - 업링크 1 옵션에서 vmnic3을 선택합니다.
   - 추가 를 클릭합니다.

> 이 구성에서는 Vmnic2 및 vmnic3이 iSCSI 부팅에 사용됩니다. ESXi 호스트에 추가 NIC가 있는 경우 vmnic 번호가 다를 수 있습니다. iSCSI 부트에 사용되는 NIC를 확인하려면 CIMC의 iSCSI vNIC의 MAC 주소를 ESXi의 vmnics와 일치시킵니다.

9. 가운데 창에서 VMkernel NIC 탭을 선택합니다.
10. Add VMkernel NIC 를 선택합니다.
    - iScosibootPG-B의 포트 그룹 이름을 새로 지정합니다.
    - 가상 스위치에 대해 iSciBootvSwitch-B를 선택합니다.
    - VLAN ID에 '<<iscsib_vlan_id>>'를 입력합니다.
    - MTU를 9000으로 변경합니다.
    - IPv4 설정 을 확장합니다.
    - 정적 설정을 선택합니다.
    - Address 에 "<<var_hosta_iscsib_ip>>"를 입력합니다.
    - 서브넷 마스크에 '<<var_hosta_iscsib_mask>>'를 입력합니다.
    - 생성 을 클릭합니다.

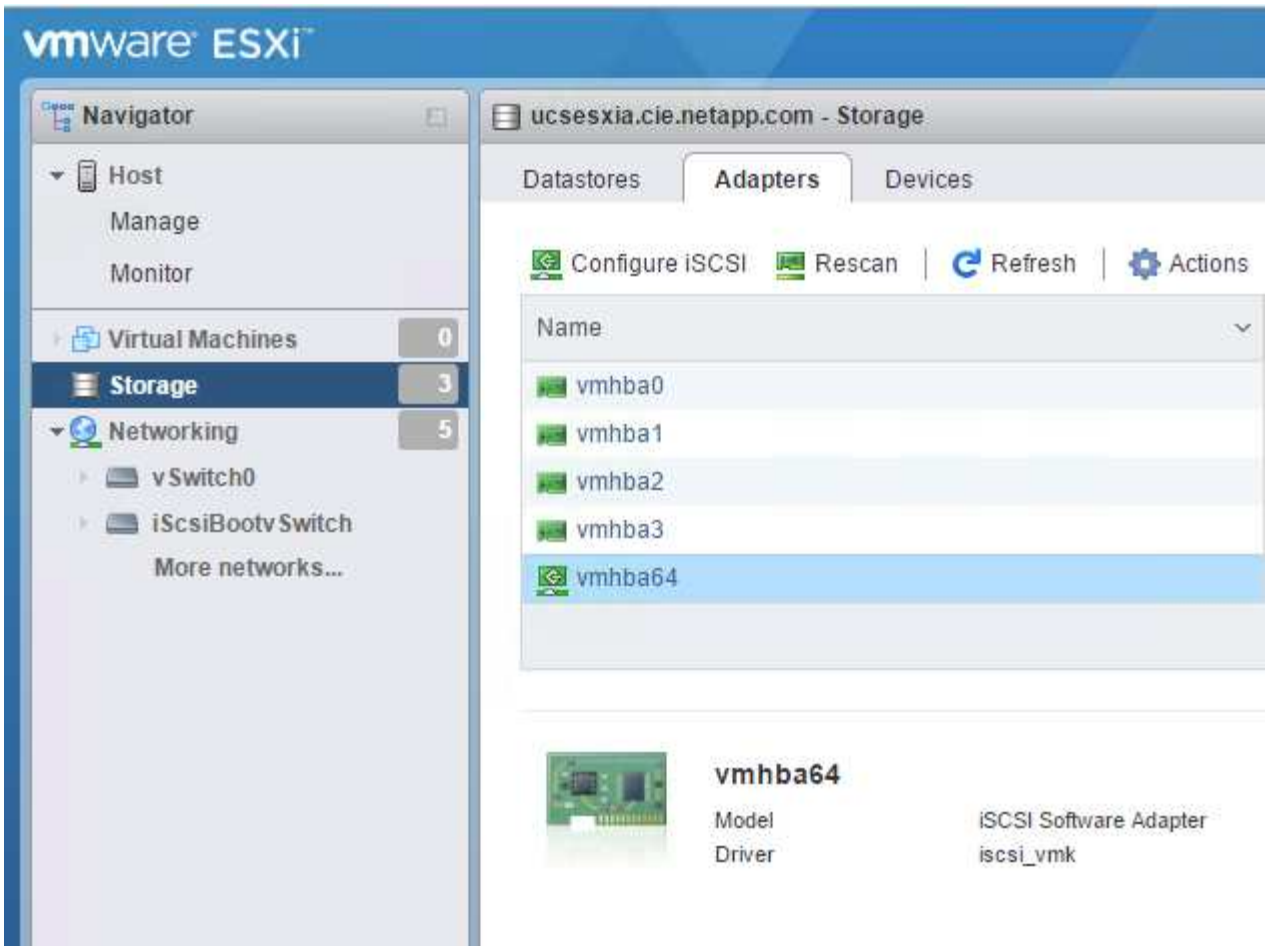


iSciBootPG-A에서 MTU를 9000으로 설정합니다

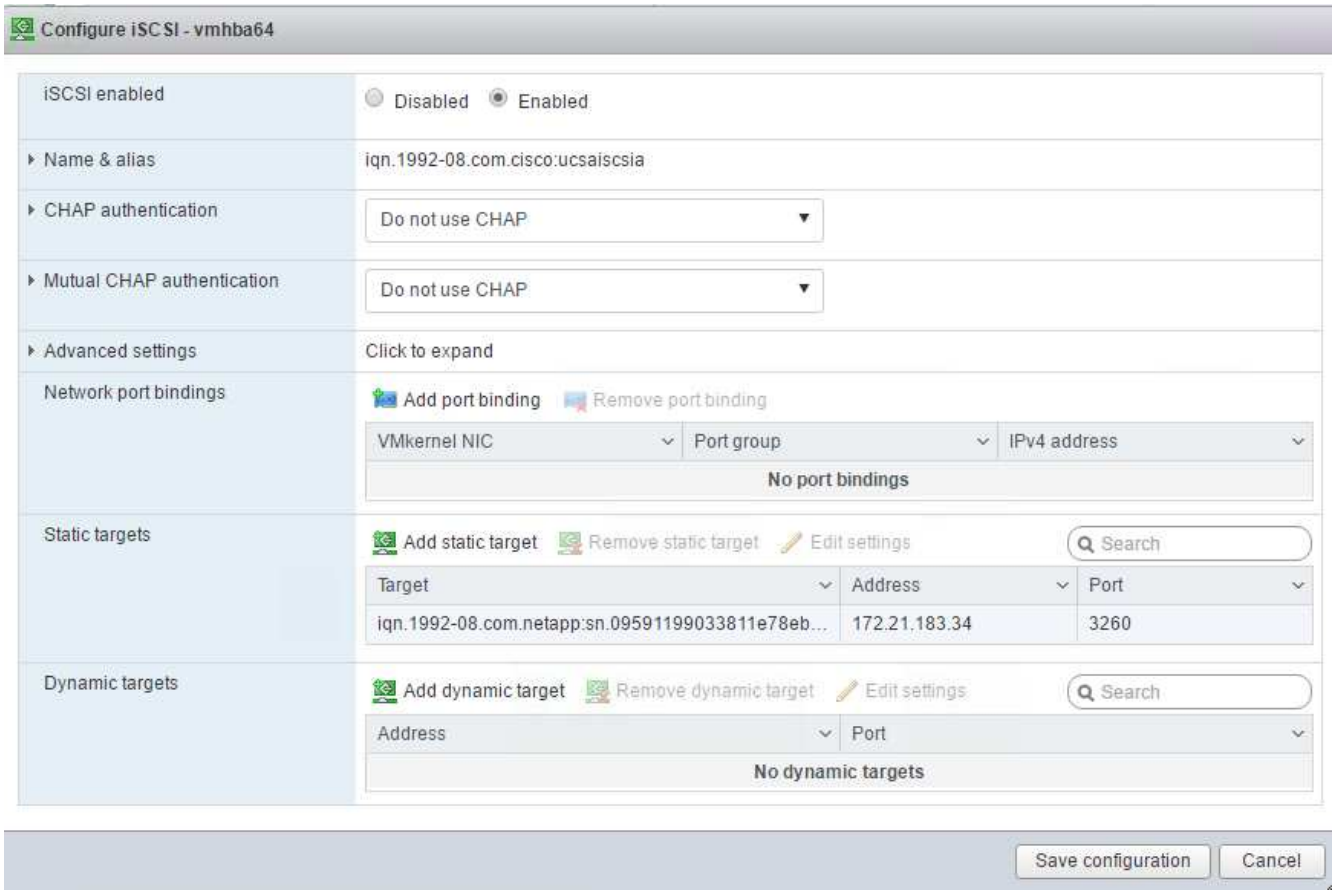
iSCSI 다중 경로를 구성합니다

ESXi 호스트에 iSCSI 다중 경로를 설정하려면 다음 단계를 수행하십시오.

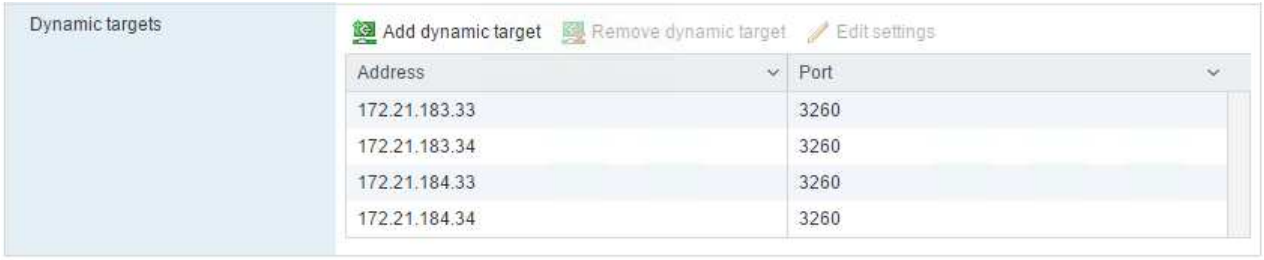
1. 왼쪽 탐색 창에서 스토리지 를 선택합니다. 어댑터를 클릭합니다.
2. iSCSI 소프트웨어 어댑터를 선택하고 iSCSI 구성 을 클릭합니다.



3. 동적 대상에서 동적 대상 추가를 클릭합니다.



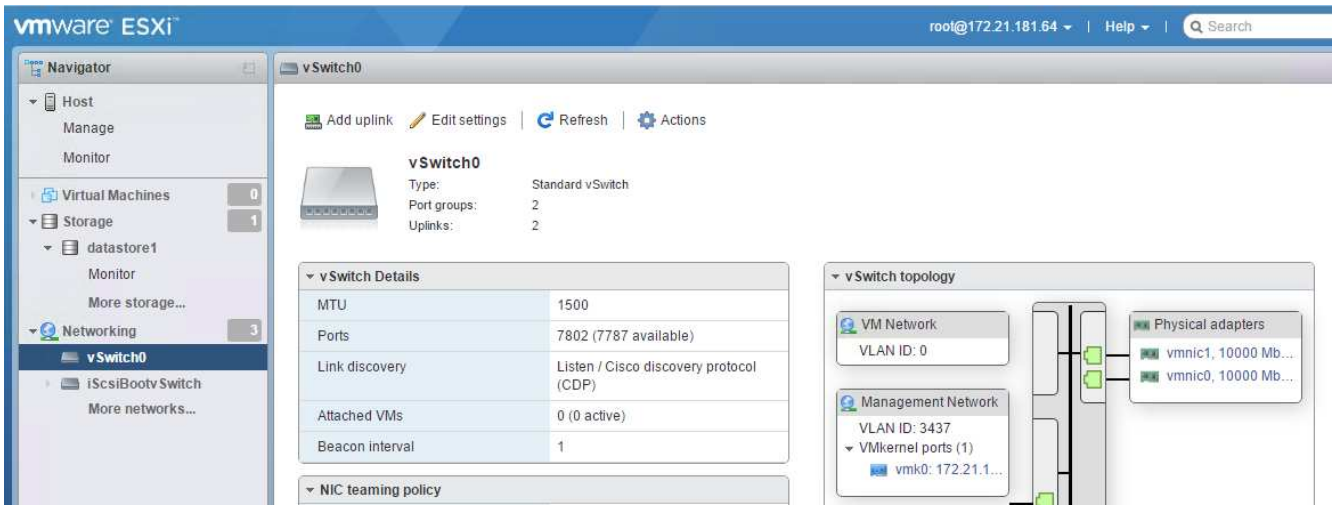
4. IP 주소 'iscsi_lif01a'를 입력합니다.
   - IP 주소 iscsi_liff 01b, iscsi_liff 02a, iscsi_liff 02b와 함께 이 과정을 반복합니다.
   - 구성 저장 을 클릭합니다.



NetApp 클러스터에서 'network interface show' 명령을 실행하거나 OnCommand System Manager에서 네트워크 인터페이스 탭을 확인하여 iSCSI LIF IP 주소를 찾을 수 있습니다.

ESXi 호스트를 구성합니다

1. 왼쪽 탐색 창에서 네트워킹 을 선택합니다.
2. vSwitch0을 선택합니다.



3. 설정 편집 을 선택합니다.
4. MTU를 9000으로 변경합니다.
5. NIC 티밍을 확장하고 vmnic0 및 vmnic1이 모두 활성으로 설정되어 있는지 확인합니다.

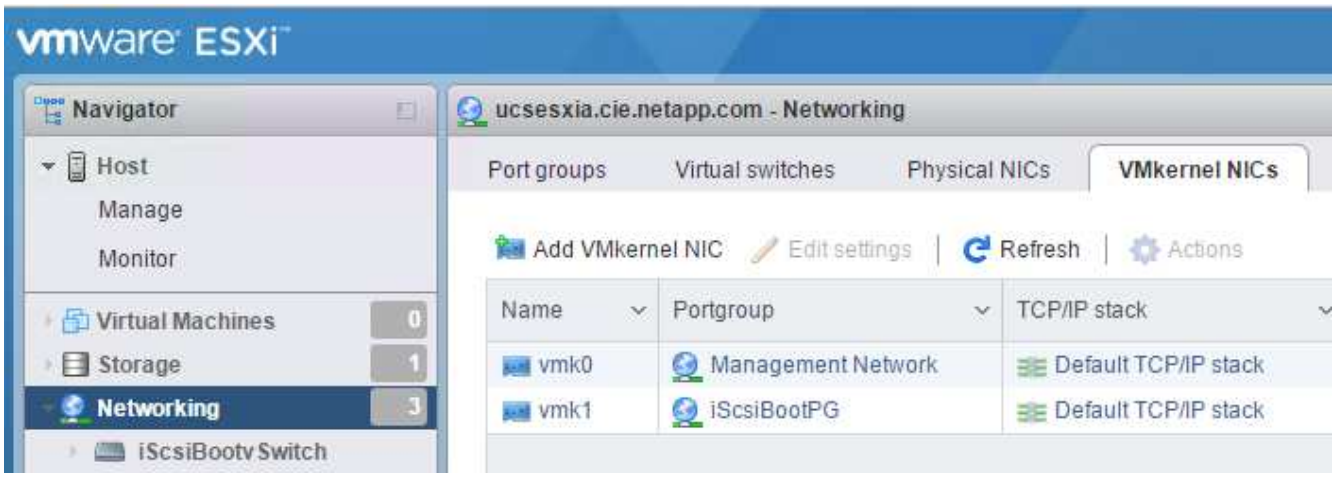
포트 그룹 및 **VMkernel NIC**를 구성합니다

1. 왼쪽 탐색 창에서 네트워킹 을 선택합니다.
2. 포트 그룹 탭을 마우스 오른쪽 단추로 클릭합니다.

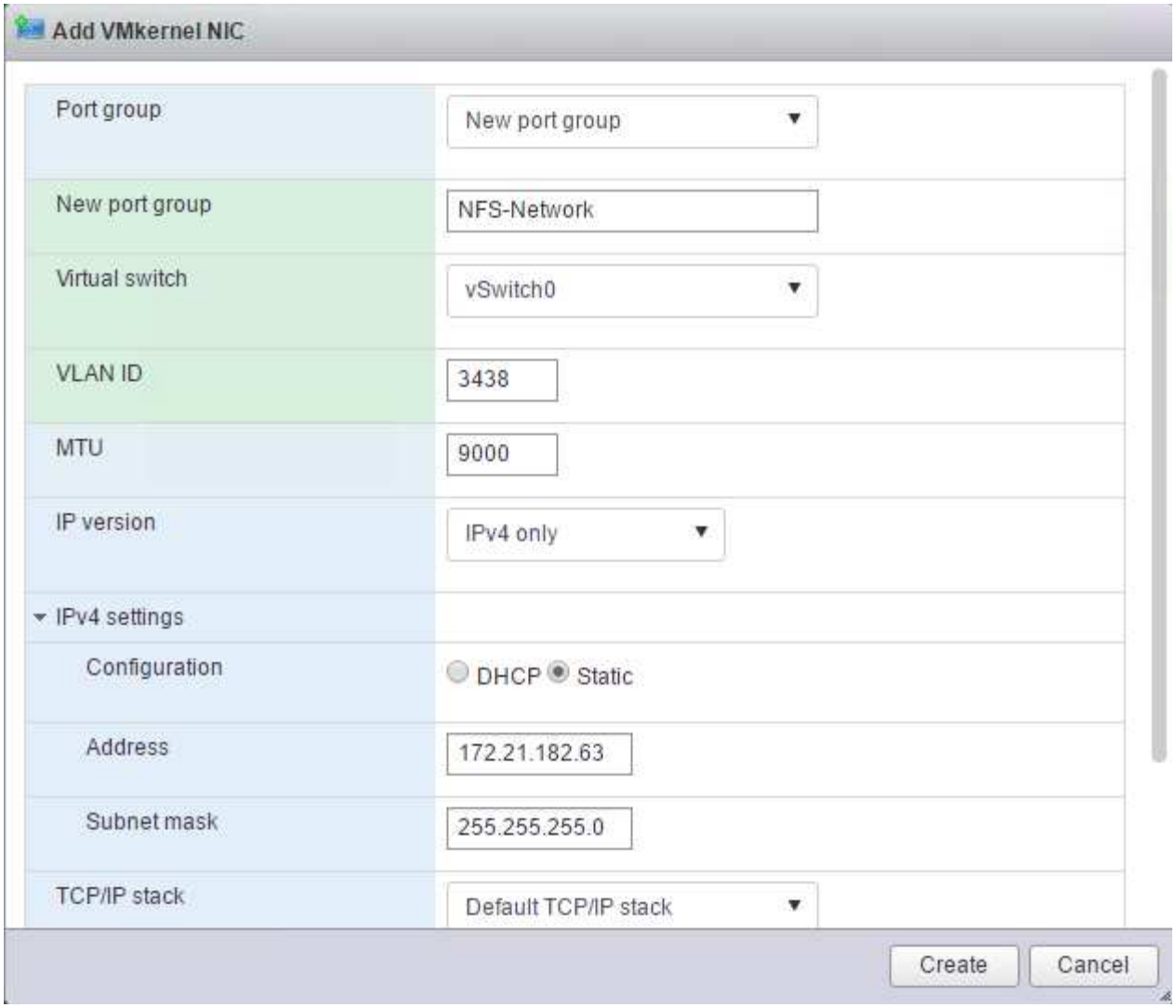
3. VM Network를 마우스 오른쪽 버튼으로 클릭하고 Edit를 선택합니다. VLAN ID를 '<<var_vm_traffic_vlan>>'로 변경합니다.
4. 포트 그룹 추가 를 클릭합니다.
   - 포트 그룹의 이름을 MGMT-Network로 지정합니다.
   - VLAN ID에 '<<mgmt_vlan>>'를 입력합니다.
   - vSwitch0이 선택되어 있는지 확인합니다.

◦ 추가 를 클릭합니다.

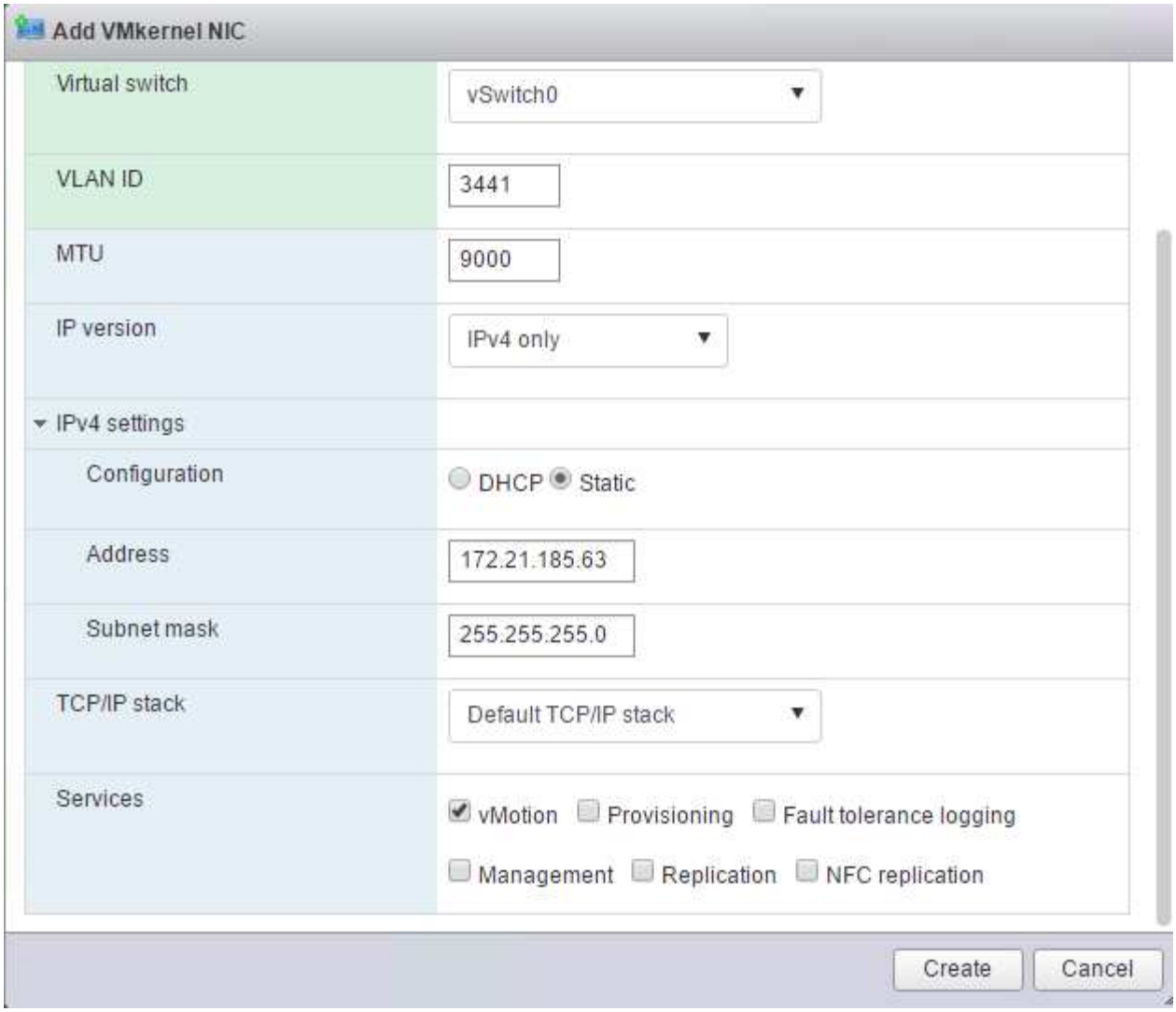
5. VMkernel NIC 탭을 클릭합니다.



6. Add VMkernel NIC 를 선택합니다.
   ◦ 새 포트 그룹을 선택합니다.
   ◦ 포트 그룹의 이름을 NFS-Network로 지정합니다.
   ◦ VLAN ID에 '<<nfs_vlan_id>>'를 입력합니다.
   ◦ MTU를 9000으로 변경합니다.
   ◦ IPv4 설정 을 확장합니다.
   ◦ 정적 설정을 선택합니다.
   ◦ Address 에 "<<var_hosta_nfs_ip>>"를 입력합니다.
   ◦ 서브넷 마스크에 '<<var_hosta_nfs_mask>>'를 입력합니다.
   ◦ 생성 을 클릭합니다.



7. 이 프로세스를 반복하여 vMotion VMkernel 포트를 생성합니다.
8. Add VMkernel NIC 를 선택합니다.
    a. 새 포트 그룹을 선택합니다.
    b. 포트 그룹의 이름을 vMotion으로 지정합니다.
    c. VLAN ID에 '\< vMotion_vlan_id>>'를 입력합니다.
    d. MTU를 9000으로 변경합니다.
    e. IPv4 설정 을 확장합니다.
    f. 정적 설정을 선택합니다.
    g. Address 에 "<<var_hosta_vmotion_ip>>"를 입력합니다.
    h. 서브넷 마스크에 '<<var_hosta_vmotion_mask>>'를 입력합니다.
    i. IPv4 설정 후 vMotion 확인란이 선택되어 있는지 확인합니다.

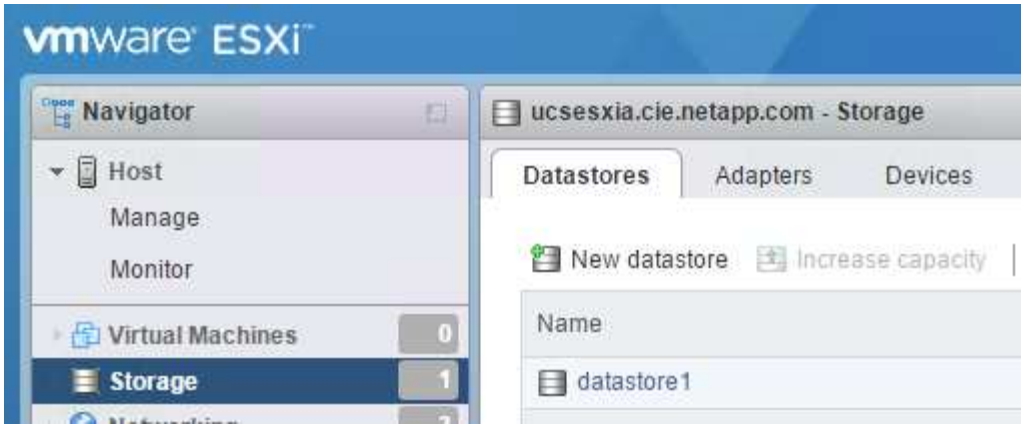


라이센싱에서 허용하는 경우 VMware vSphere 분산 스위치를 사용하는 등 여러 가지 방법으로 ESXi 네트워킹을 구성할 수 있습니다. 비즈니스 요구 사항을 충족하는 데 필요한 경우 FlexPod Express에서 대체 네트워크 구성이 지원됩니다.

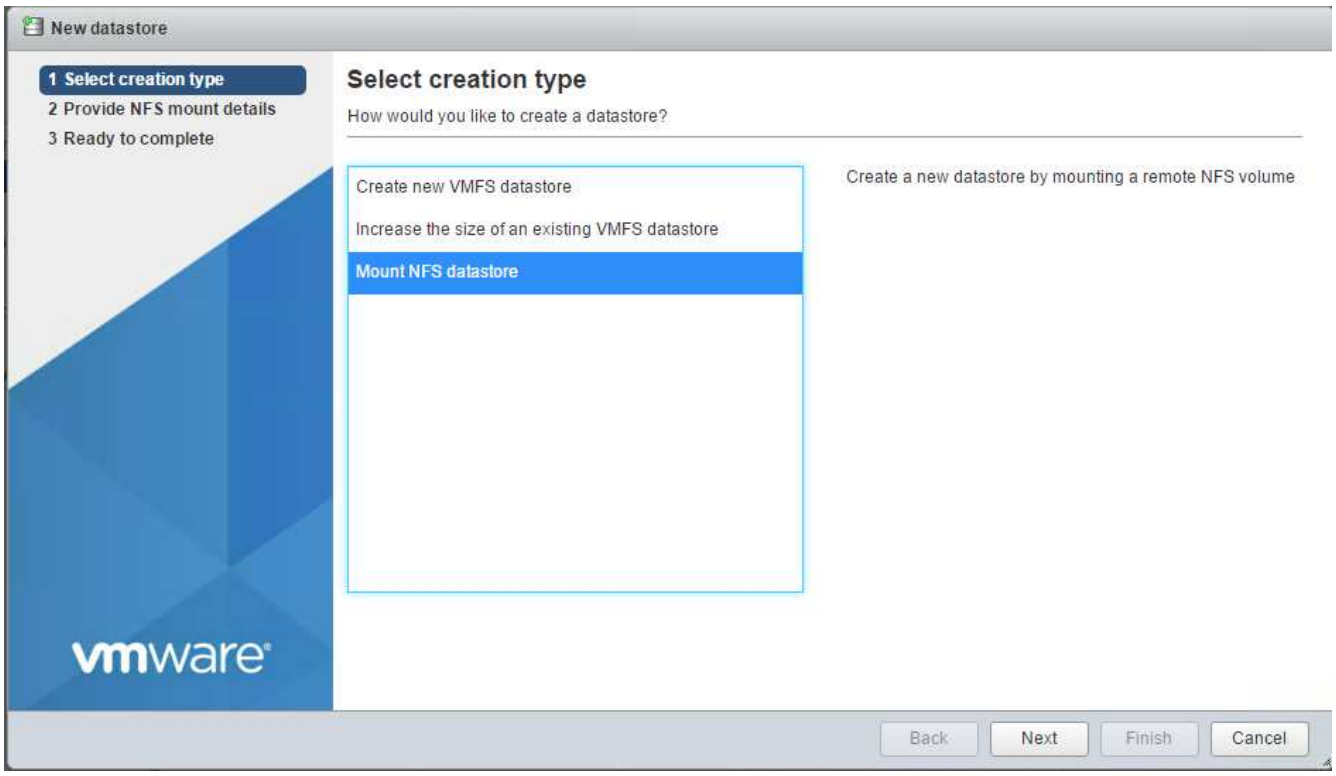
첫 번째 데이터 저장소를 마운트합니다

마운트할 첫 번째 데이터 저장소는 가상 머신용 infra_datastore_1 데이터 저장소와 가상 머신 스왑 파일용 infra_swap 데이터 저장소입니다.

1. 왼쪽 탐색 창에서 스토리지 를 클릭한 다음 새 데이터 저장소 를 클릭합니다.



2. Mount NFS Datastore를 선택합니다.



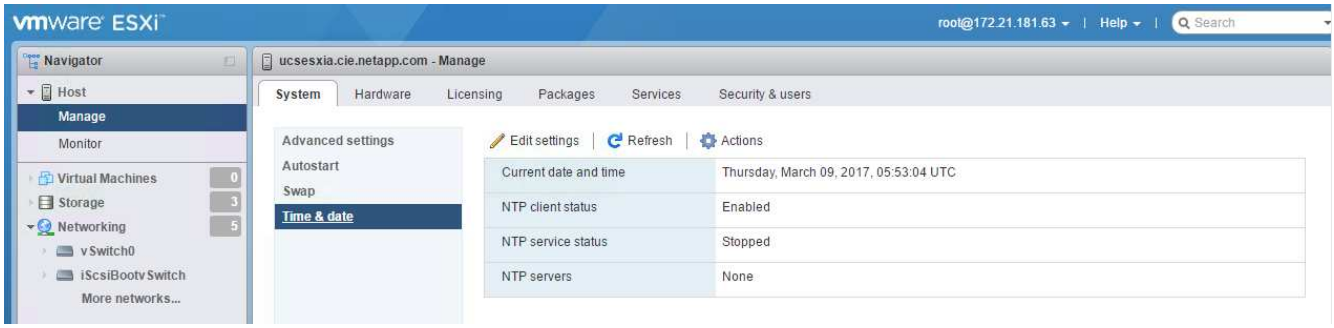
3. 그런 다음 NFS 마운트 세부 정보 제공 페이지에 다음 정보를 입력합니다.
   - 이름: 'infra_datastore_1'
   - NFS 서버:\<<var_NodeA_nfs_lif>'
   - 공유:/infra_datastore_1
   - NFS 3이 선택되어 있는지 확인합니다.
4. 마침 을 클릭합니다. 최근 작업 창에서 작업이 완료된 것을 볼 수 있습니다.
5. 다음 프로세스를 반복하여 infra_swap 데이터 저장소를 마운트합니다.
   - 이름: infra_swap
   - NFS 서버:\<<var_NodeA_nfs_lif>'
   - 공유: '/infra_swap'

◦ NFS 3이 선택되어 있는지 확인합니다.

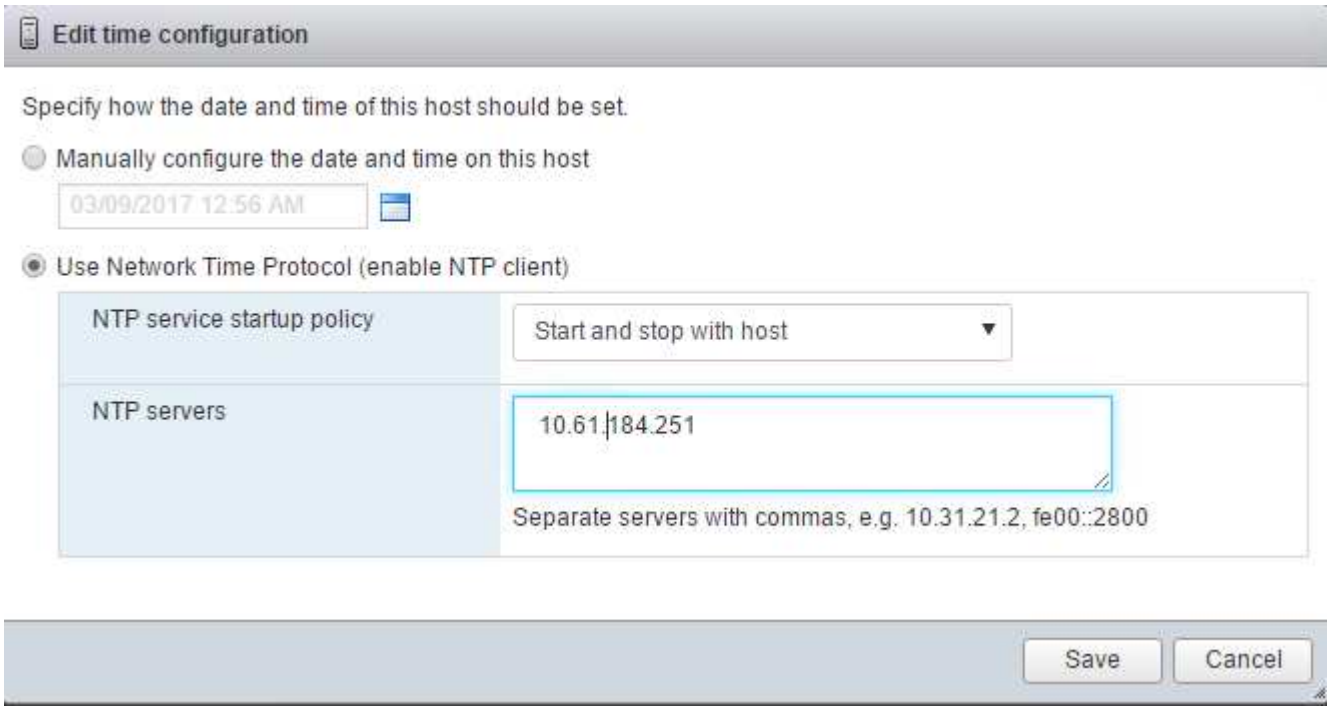
NTP를 구성합니다

ESXi 호스트에 대해 NTP를 구성하려면 다음 단계를 수행하십시오.

1. 왼쪽 탐색 창에서 관리 를 클릭합니다. 오른쪽 창에서 시스템 을 선택한 다음 시간 및 날짜 를 클릭합니다.



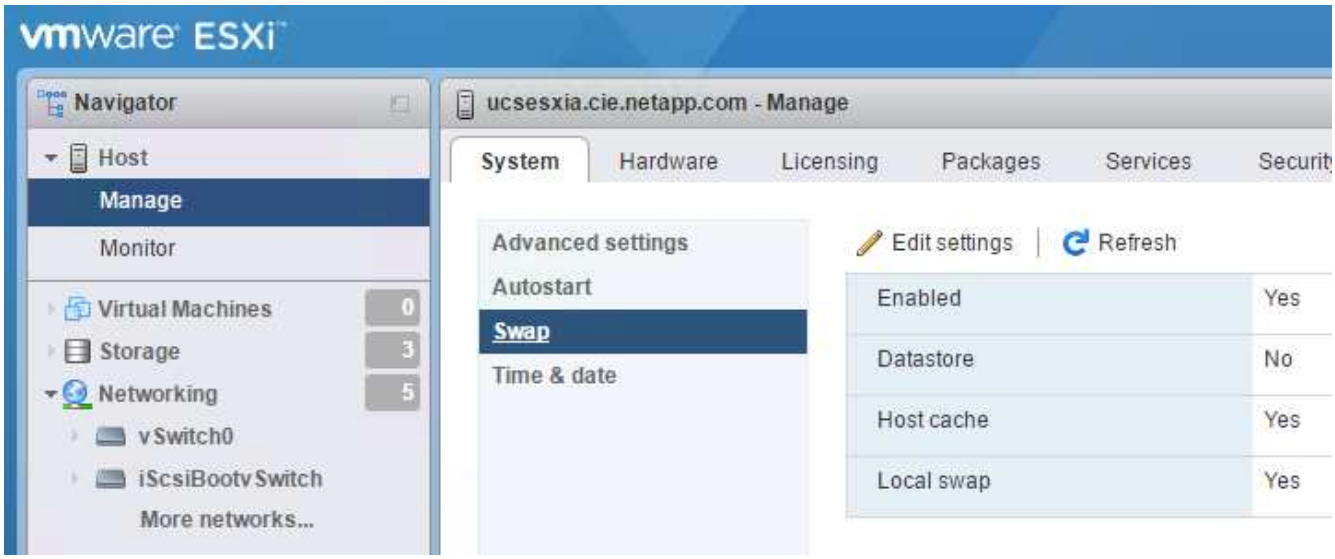
2. Use Network Time Protocol (Enable NTP Client) 을 선택합니다.
3. Start and Stop with Host 를 NTP 서비스 시작 정책으로 선택합니다.
4. NTP 서버로 '<<var_ntp>>'를 입력합니다. 여러 NTP 서버를 설정할 수 있습니다.
5. 저장 을 클릭합니다.



가상 머신 스왑 파일 위치를 이동합니다

다음 단계에서는 가상 머신 스왑 파일 위치를 이동하는 방법을 자세히 설명합니다.

1. 왼쪽 탐색 창에서 관리 를 클릭합니다. 오른쪽 창에서 시스템을 선택한 다음 바꾸기를 클릭합니다.



2. 설정 편집 을 클릭합니다. Datastore 옵션에서 infra_swap을 선택합니다.

3. 저장 을 클릭합니다.

VMware VAAI용 **NetApp NFS** 플러그인 **1.0.20**을 설치합니다

VMware VAAI용 NetApp NFS 플러그인 1.0.20을 설치하려면 다음 단계를 완료하십시오.

1. 다음 명령을 입력하여 VAAI가 활성화되었는지 확인합니다.

```
esxcfg-advcfg -g /DataMover/HardwareAcceleratedMove
esxcfg-advcfg -g /DataMover/HardwareAcceleratedInit
```

VAAI가 활성화된 경우 다음 명령을 실행하면 다음 출력이 생성됩니다.

```
~ #  esxcfg-advcfg -g /DataMover/HardwareAcceleratedMove
Value of HardwareAcceleratedMove is 1
~ # esxcfg-advcfg -g /DataMover/HardwareAcceleratedInit
Value of HardwareAcceleratedInit is 1
```

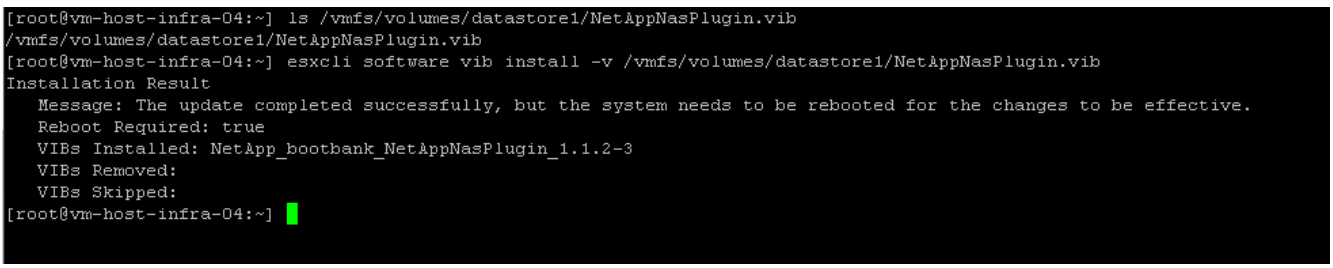
2. VAAI가 설정되어 있지 않으면 다음 명령을 입력하여 VAAI를 사용하도록 설정합니다.

```
esxcfg-advcfg -s 1 /DataMover/HardwareAcceleratedInit
esxcfg-advcfg -s 1 /DataMover/HardwareAcceleratedMove
```

이러한 명령은 다음과 같은 출력을 생성합니다.

```
~ # esxcfg-advcfg -s 1 /Data Mover/HardwareAcceleratedInit
Value of HardwareAcceleratedInit is 1
~ #  esxcfg-advcfg -s 1 /DataMover/HardwareAcceleratedMove
Value of HardwareAcceleratedMove is 1
```

3. NetApp NFS Plug-in for VMware VAAI 다운로드:
   a. 로 이동합니다 "소프트웨어 다운로드 페이지".
   b. 아래로 스크롤하여 VMware VAAI용 NetApp NFS 플러그인 을 클릭합니다.
   c. ESXi 플랫폼을 선택합니다.
   d. 최신 플러그인의 오프라인 번들(.zip) 또는 온라인 번들(.vib)을 다운로드합니다.
4. ESX CLI를 사용하여 ESXi 호스트에 플러그인을 설치합니다.
5. ESXi 호스트를 재부팅합니다.



"다음: VMware vCenter Server 6.7을 설치합니다"

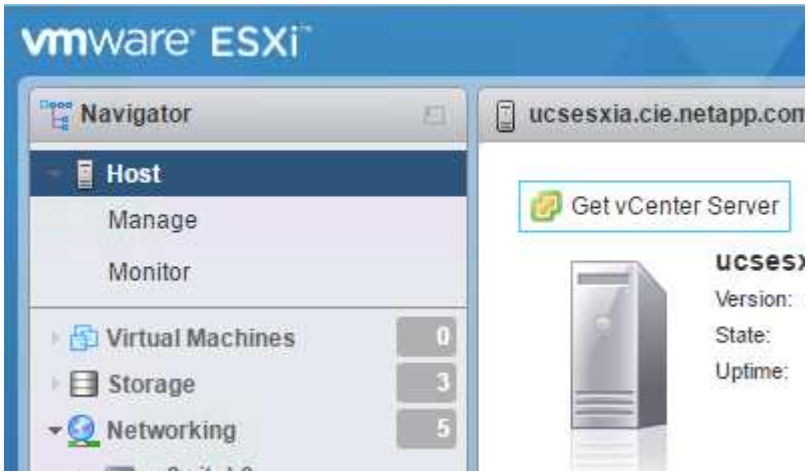
VMware vCenter Server 6.7을 설치합니다

이 섹션에서는 FlexPod Express 구성에 VMware vCenter Server 6.7을 설치하는 절차를 자세히 설명합니다.

FlexPod Express는 VCSA(VMware vCenter Server Appliance)를 사용합니다.

VMware vCenter Server 어플라이언스를 다운로드합니다

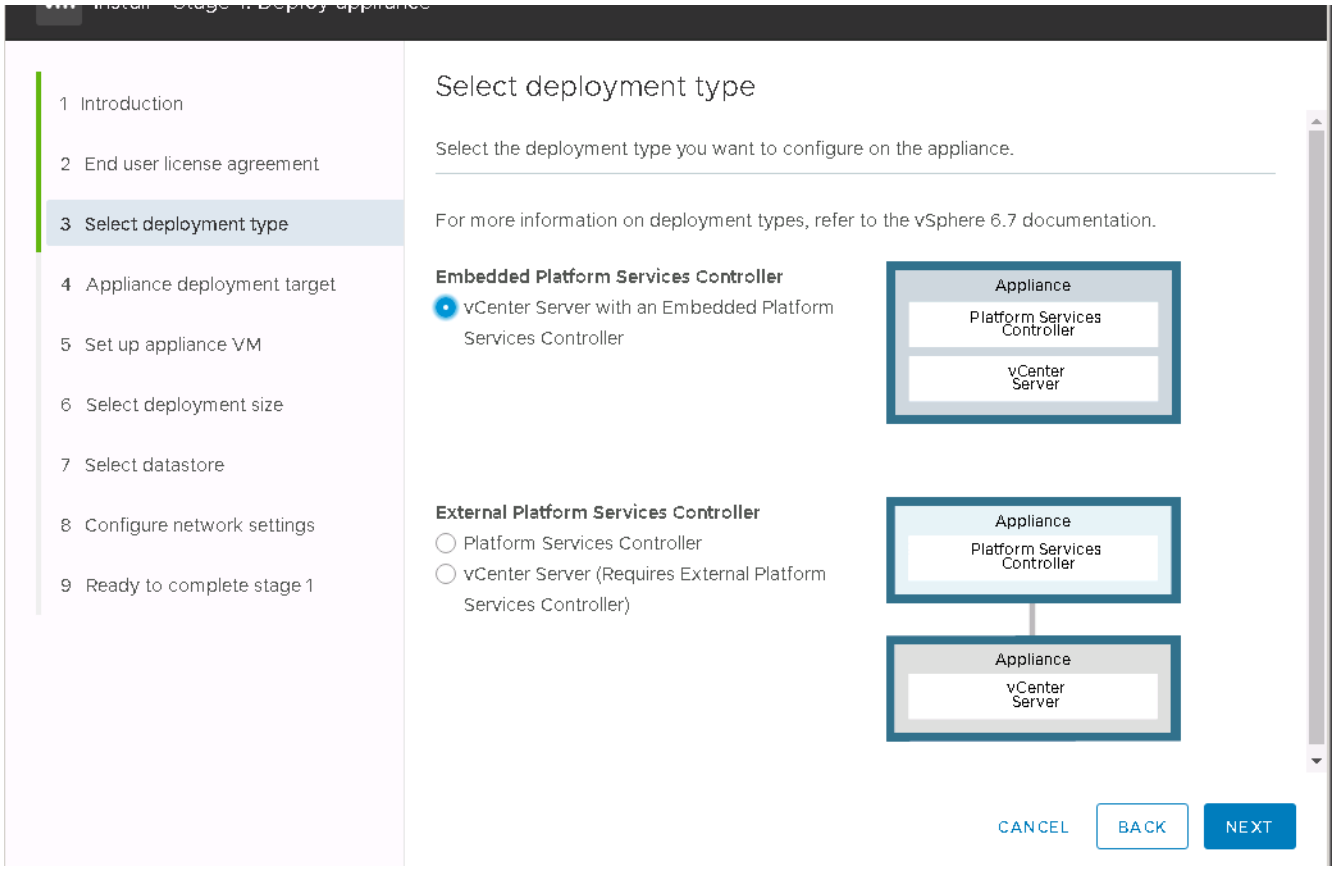
1. VCSA를 다운로드합니다. ESXi 호스트를 관리할 때 vCenter Server 가져오기 아이콘을 클릭하여 다운로드 링크를 액세스합니다.



2. VMware 사이트에서 VCSA를 다운로드합니다.

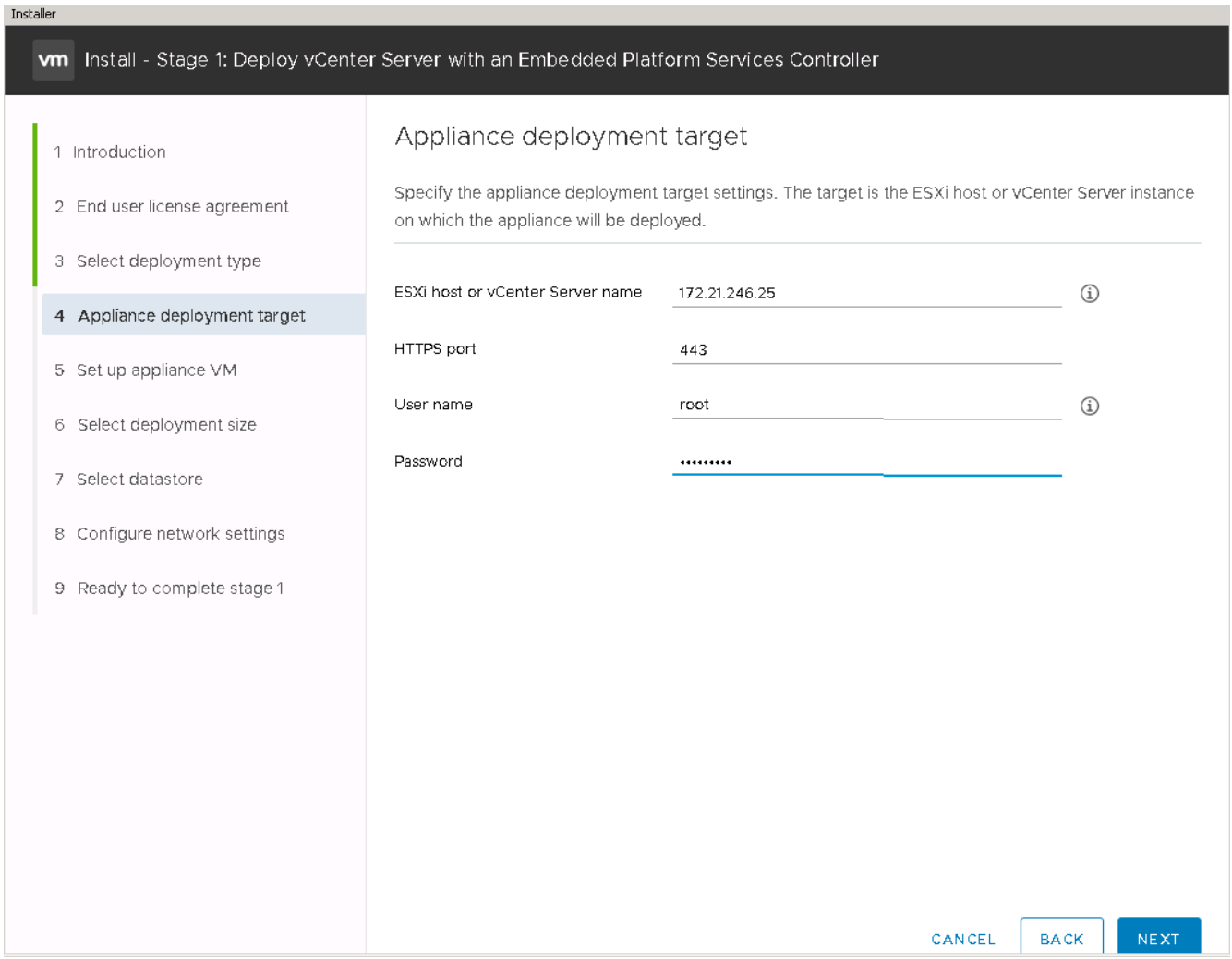
> Microsoft Windows vCenter Server 설치 가능한 가 지원되지만 VMware는 새로운 구축에 VCSA를 권장합니다.

3. ISO 이미지를 마운트합니다.
4. vcsa-UI-installer> Win32 디렉터리로 이동합니다. installer.exe를 두 번 클릭합니다.
5. 설치 를 클릭합니다.
6. 소개 페이지에서 다음 을 클릭합니다.
7. 최종 사용자 라이센스 계약에 동의합니다.
8. 배포 유형으로 임베디드 플랫폼 서비스 컨트롤러 를 선택합니다.

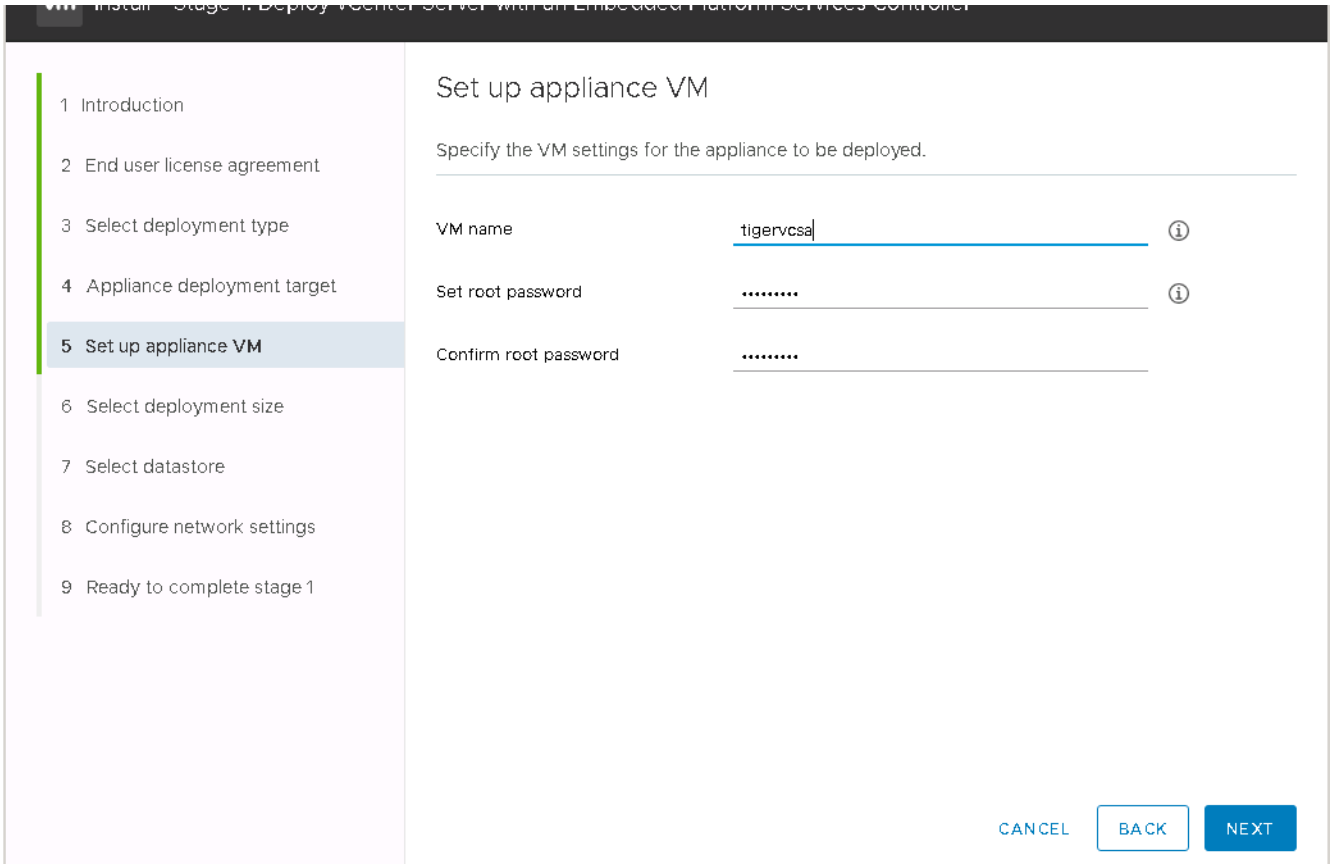


필요한 경우 외부 플랫폼 서비스 컨트롤러 배포도 FlexPod Express 솔루션의 일부로 지원됩니다.

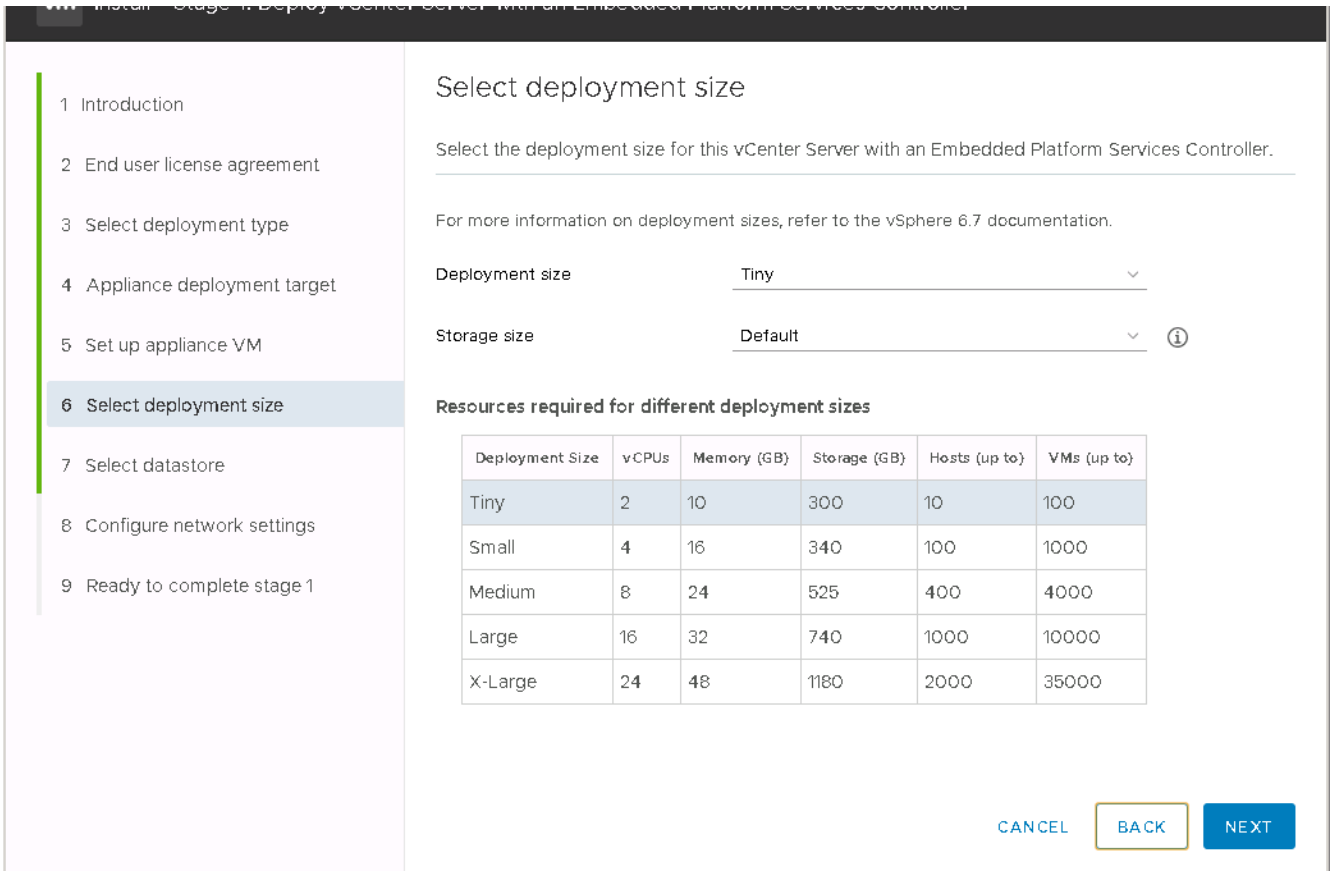
9. Appliance Deployment Target에서 구축한 ESXi 호스트의 IP 주소와 루트 사용자 이름 및 루트 암호를 입력합니다.



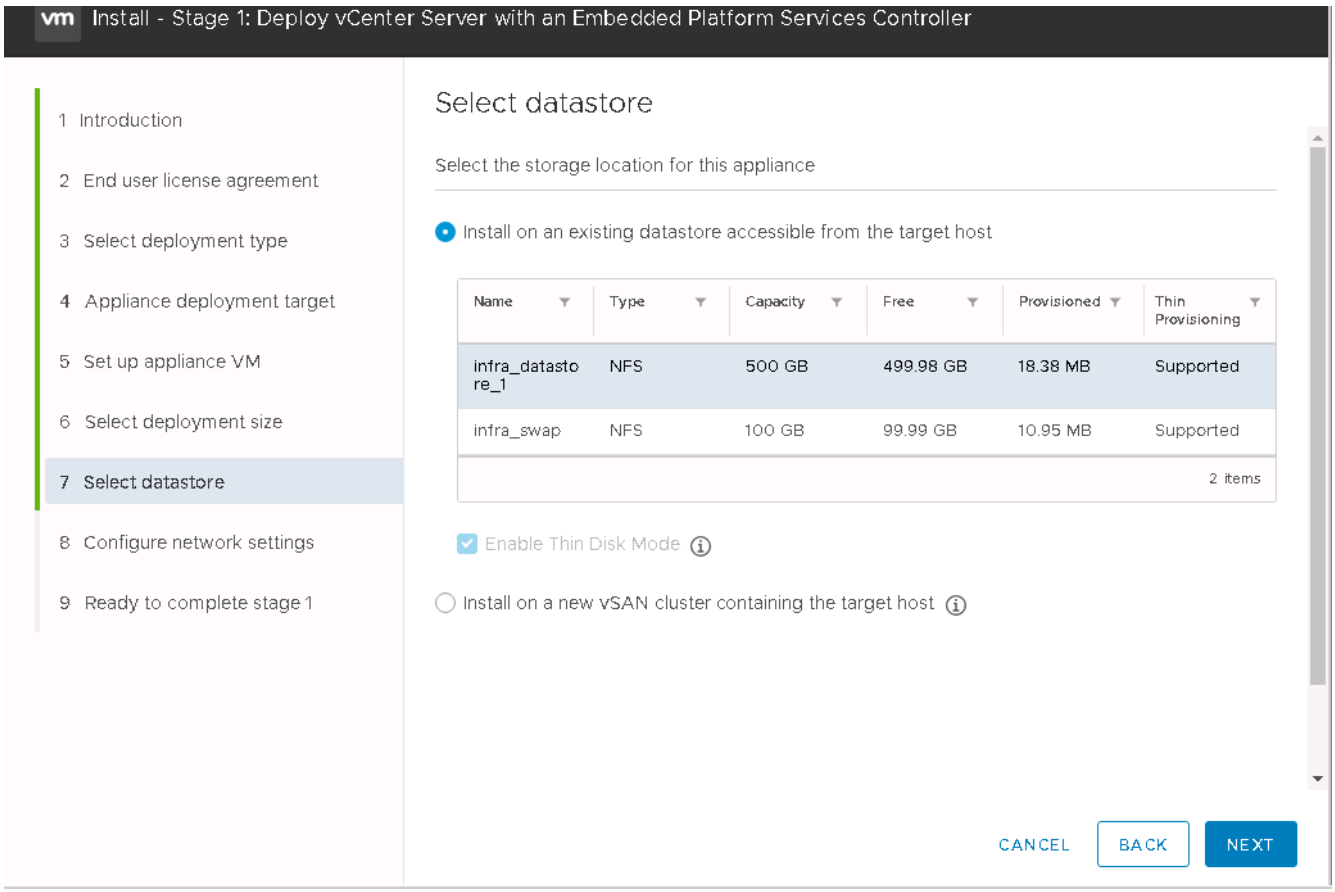
10. VCSA에 사용할 VM 이름과 루트 암호를 VCSA로 입력하여 어플라이언스 VM을 설정합니다.



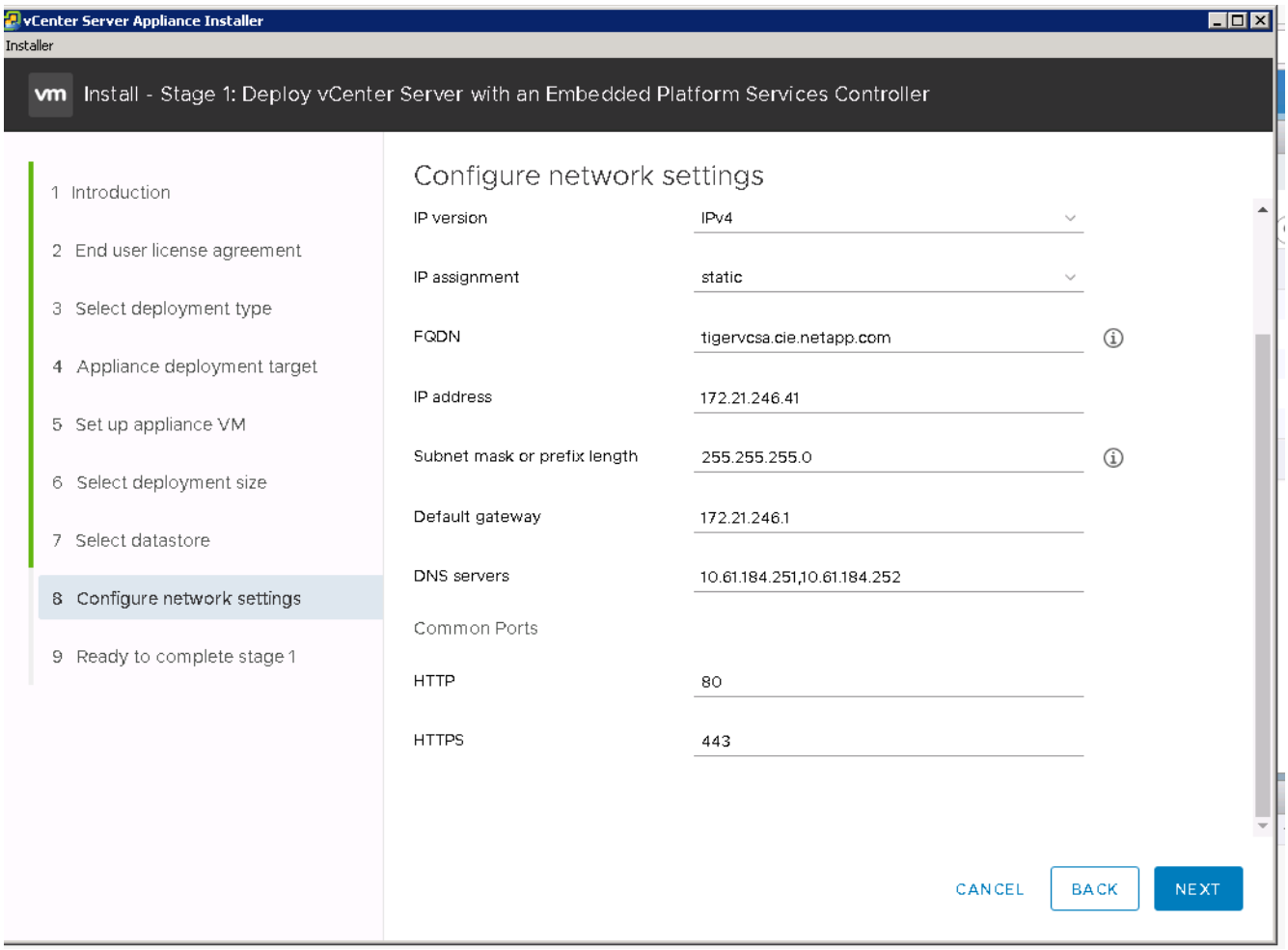
11. 환경에 가장 적합한 구축 크기를 선택합니다. 다음 을 클릭합니다.



12. infra_datastore_1 데이터 저장소를 선택합니다. 다음 을 클릭합니다.

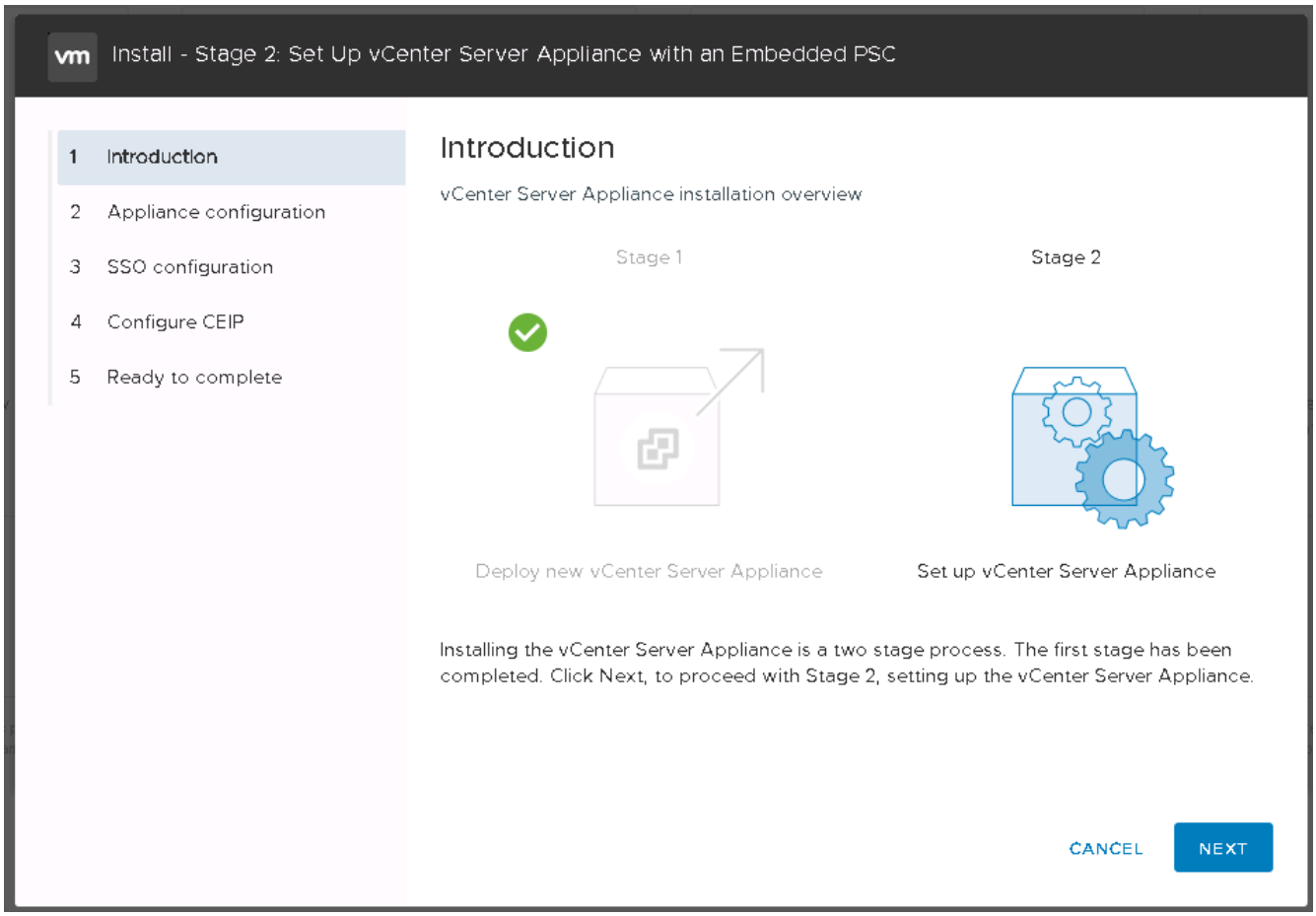


13. 네트워크 설정 구성 페이지에 다음 정보를 입력하고 다음 을 클릭합니다.
    a. Network 에서 MGMT-Network 를 선택합니다.
    b. VCSA에 사용할 FQDN 또는 IP를 입력합니다.
    c. 사용할 IP 주소를 입력합니다.
    d. 사용할 서브넷 마스크를 입력합니다.
    e. 기본 게이트웨이를 입력합니다.
    f. DNS 서버를 입력합니다.
14. 1단계 완료 준비 페이지에서 입력한 설정이 올바른지 확인합니다. 마침 을 클릭합니다.



VCSA가 지금 설치됩니다. 이 과정은 몇 분 정도 소요됩니다.

15. 1단계가 완료되면 완료되었다는 메시지가 나타납니다. 계속 을 클릭하여 2단계 구성을 시작합니다.
16. 2단계 소개 페이지에서 다음 을 클릭합니다.



17. NTP 서버 주소에 대해 '<<var_ntp_id>>'를 입력합니다. 여러 NTP IP 주소를 입력할 수 있습니다.

    vCenter Server HA(고가용성)를 사용하려는 경우 SSH 액세스가 설정되어 있는지 확인합니다.

18. SSO 도메인 이름, 암호 및 사이트 이름을 구성합니다. 다음 을 클릭합니다.

    특히 vSphere.local 도메인 이름을 벗어난 경우 이러한 값을 참조로 기록합니다.

19. 원하는 경우 VMware 고객 경험 프로그램에 참여하십시오. 다음 을 클릭합니다.
20. 설정 요약을 봅니다. 마침 을 클릭하거나 뒤로 단추를 사용하여 설정을 편집합니다.
21. 설치가 시작된 후 설치를 일시 중지하거나 중지할 수 없다는 메시지가 나타납니다. 계속하려면 확인을 클릭하십시오.

    어플라이언스 설정이 계속됩니다. 이 작업은 몇 분 정도 걸립니다.

    설정이 성공했음을 나타내는 메시지가 나타납니다.

    vCenter Server에 액세스하기 위해 설치 관리자가 제공하는 링크를 클릭할 수 있습니다.

"다음: VMware vCenter Server 6.7 및 vSphere 클러스터링을 구성합니다."

VMware vCenter Server 6.7 및 **vSphere** 클러스터링 구성

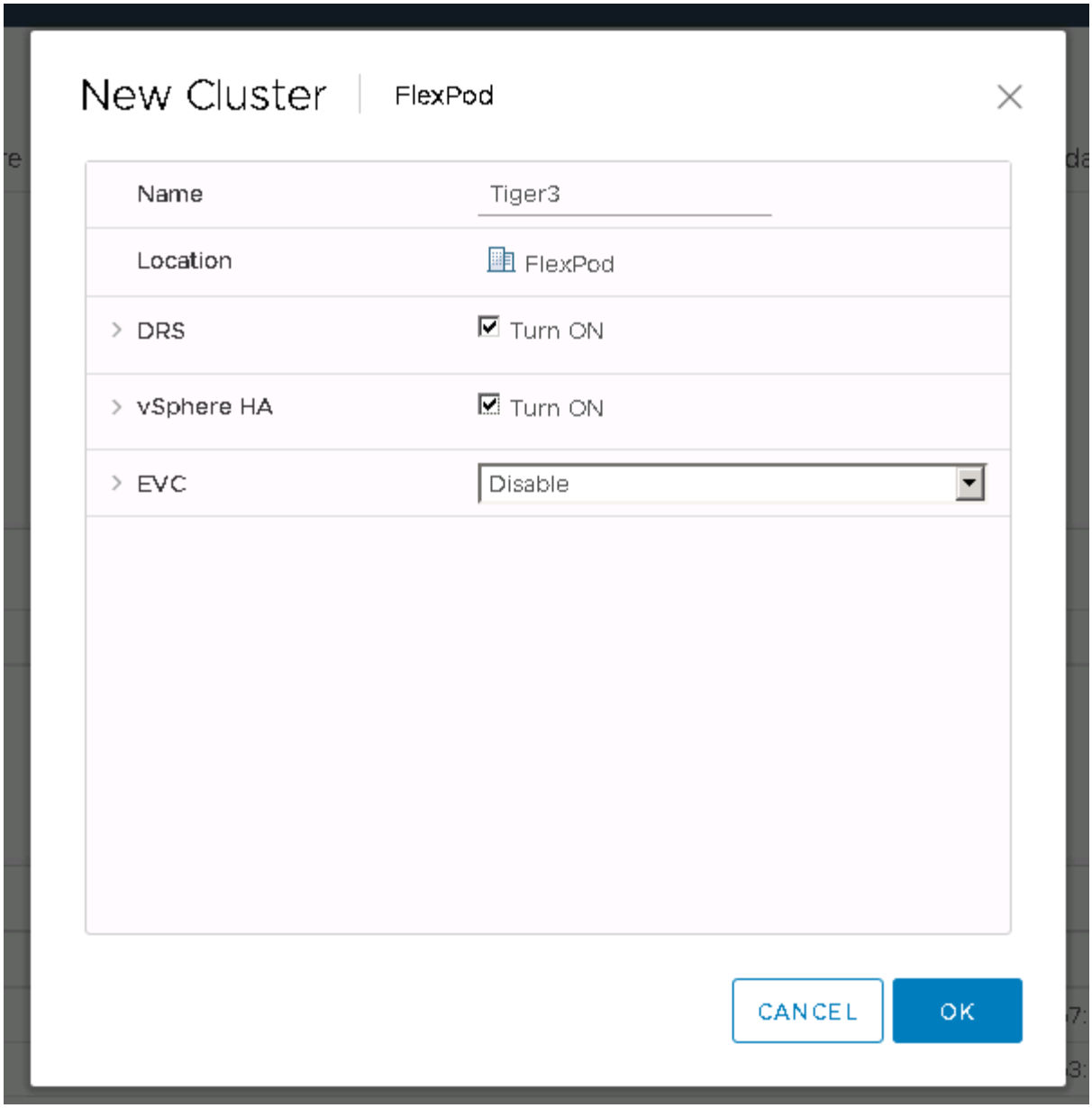
VMware vCenter Server 6.7 및 vSphere 클러스터링을 구성하려면 다음 단계를 수행하십시오.

1. https://\<<FQDN 또는 vCenter의 IP >>/vSphere-client/로 이동합니다.
2. vSphere Client 시작 을 클릭합니다.
3. 사용자 이름 mailto:administrator@vspehre.loca l[administrator@vsphere.loca l^]과 VCSA 설정 프로세스 중에 입력한 SSO 암호를 사용하여 로그인합니다.
4. vCenter 이름을 마우스 오른쪽 버튼으로 클릭하고 New Datacenter를 선택합니다.
5. 데이터 센터의 이름을 입력하고 확인 을 클릭합니다.

vSphere 클러스터를 생성합니다

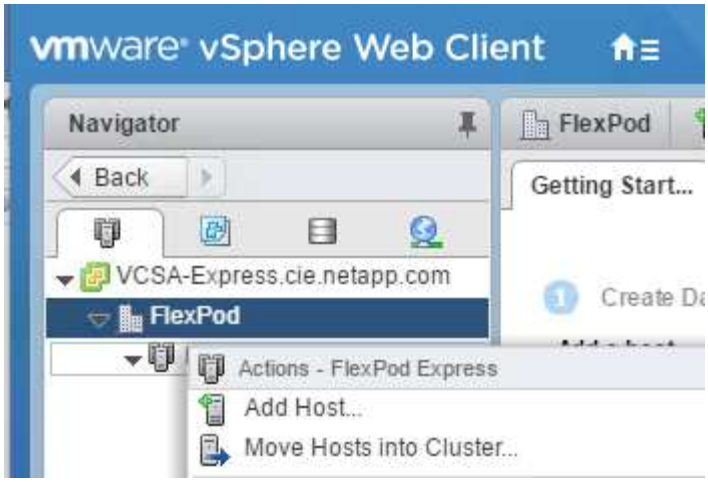
vSphere 클러스터를 생성하려면 다음 단계를 수행하십시오.

1. 새로 생성된 데이터 센터를 마우스 오른쪽 버튼으로 클릭하고 New Cluster를 선택합니다.
2. 클러스터의 이름을 입력합니다.
3. 확인란을 선택하여 DR 및 vSphere HA를 설정합니다.
4. 확인 을 클릭합니다.



클러스터에 **ESXi** 호스트를 추가합니다

1. 클러스터를 마우스 오른쪽 버튼으로 클릭하고 Add Host를 선택합니다.



2. 클러스터에 ESXi 호스트를 추가하려면 다음 단계를 수행하십시오.
   a. 호스트의 IP 또는 FQDN을 입력합니다. 다음 을 클릭합니다.
   b. 루트 사용자 이름과 암호를 입력합니다. 다음 을 클릭합니다.
   c. 예를 클릭하여 호스트의 인증서를 VMware 인증서 서버에서 서명한 인증서로 바꿉니다.
   d. 호스트 요약 페이지에서 다음 을 클릭합니다.
   e. 녹색 + 아이콘을 클릭하여 vSphere 호스트에 라이센스를 추가합니다.

      이 단계는 원할 경우 나중에 완료할 수 있습니다.

   f. 다음 을 클릭하여 잠금 모드를 해제합니다.
   g. VM 위치 페이지에서 다음 을 클릭합니다.
   h. 완료 준비 페이지를 검토합니다. 뒤로 단추를 사용하여 변경하거나 마침 을 선택합니다.
3. Cisco UCS 호스트 B에 대해 1단계와 2단계를 반복합니다 FlexPod Express 구성에 추가된 모든 호스트에 대해 이 프로세스를 완료해야 합니다.

ESXi 호스트에서 코어 덤프를 구성합니다

1. SSH를 사용하여 관리 IP ESXi 호스트에 연결하고 사용자 이름에 root를 입력한 다음 루트 암호를 입력합니다.
2. 다음 명령을 실행합니다.

```
esxcli system coredump network set -i ip_address_of_core_dump_collector
-v vmk0 -o 6500
esxcli system coredump network set --enable=true
esxcli system coredump network check
```

3. 최종 명령어를 입력하면 확인된 netdump server가 실행 중인 것으로 확인되었다는 메시지가 나타난다.

FlexPod Express에 추가된 모든 호스트에 대해 이 프로세스를 완료해야 합니다.

결론

FlexPod Express는 업계 최고의 구성요소를 사용하는 검증된 설계를 통해 간단하고 효율적인 솔루션을 제공합니다. FlexPod Express는 추가 구성요소를 추가하여 특정 비즈니스 요구사항에 맞게 확장할 수 있습니다. FlexPod Express는 전용 솔루션이 필요한 중소기업, ROBO 및 기타 기업을 염두에 두고 설계되었습니다.

추가 정보를 찾을 수 있는 위치

이 문서에 설명된 정보에 대한 자세한 내용은 다음 문서 및/또는 웹 사이트를 참조하십시오.

- NetApp 제품 설명서

  "http://docs.netapp.com"

- FlexPod Express with VMware vSphere 6.7 및 NetApp AFF A220 설계 가이드 를 참조하십시오

  "https://www.netapp.com/us/media/nva-1125-design.pdf"

직접 연결 IP 기반 스토리지를 사용하는 VMware vSphere 6.7U1 및 NetApp AFF A220을 지원하는 FlexPod Express

NVA-1131-deploy: VMware vSphere 6.7U1 및 NetApp AFF A220을 지원하는 FlexPod Express(직접 연결 IP 기반 스토리지 포함

NetApp, 스리랑카 Sree Lakshmi

업계 동향에 따르면 많은 데이터 센터가 공유 인프라 및 클라우드 컴퓨팅으로 전환하고 있습니다. 또한 기업에서는 데이터 센터에 친숙한 기술을 활용하여 원격 사무소 및 지사를 위한 간편하고 효율적인 솔루션을 찾고 있습니다.

FlexPod Express는 Cisco UCS(Cisco Unified Computing System), Cisco Nexus 스위치 제품군, NetApp 스토리지 기술을 기반으로 사전 설계되며 모범 사례 아키텍처입니다. FlexPod 익스프레스 시스템의 구성요소는 FlexPod 데이터 센터와 비슷하기 때문에 더 작은 규모로 전체 IT 인프라 환경에서 관리 시너지 효과를 실현할 수 있습니다. FlexPod 데이터 센터와 FlexPod Express는 가상화와 베어 메탈 OS와 엔터프라이즈 워크로드를 위한 최적의 플랫폼입니다.

FlexPod 데이터 센터 및 FlexPod 익스프레스 는 기본 구성을 제공하며 다양한 사용 사례와 요구 사항을 수용할 수 있도록 크기를 조정할 수 있는 다기능성을 제공합니다. 기존 FlexPod 데이터 센터 고객은 익숙한 툴을 사용하여 FlexPod 익스프레스 시스템을 관리할 수 있습니다. 새로운 FlexPod Express 고객은 환경 확장에 따라 FlexPod 데이터 센터 관리에 쉽게 적응할 수 있습니다.

FlexPod Express는 원격 사무소 및 지사(ROBO)와 중소 기업 및 중견 기업을 위한 최적의 인프라 기반입니다. 전용 워크로드에 대한 인프라를 제공하려는 고객에게 최적의 솔루션입니다.

FlexPod Express는 거의 모든 워크로드에 적합한 관리하기 쉬운 인프라를 제공합니다.

솔루션 개요

이 FlexPod Express 솔루션은 FlexPod 통합 인프라 프로그램의 일부입니다.

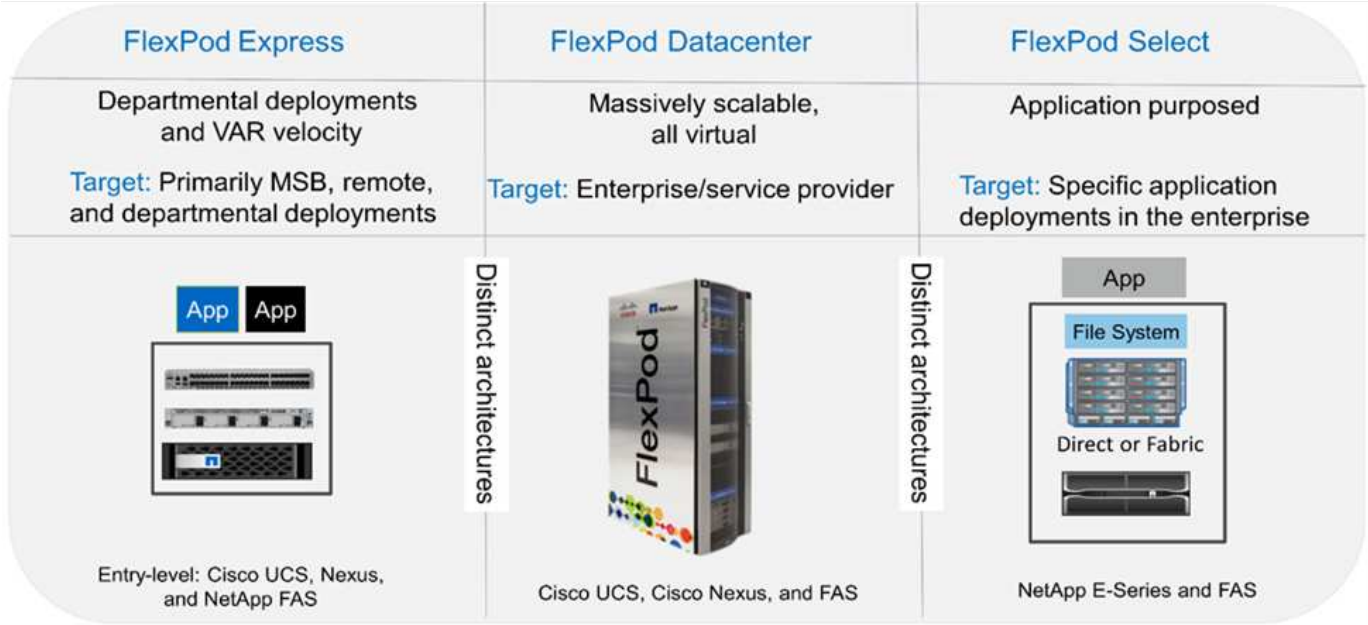
FlexPod 통합 인프라 프로그램

FlexPod 참조 아키텍처는 CVD(Cisco Validated Design) 또는 NVA(NetApp Verified Architecture)로 제공됩니다. 지정된 CVD 또는 NVA의 고객 요구 사항에 따른 편차는 이러한 변형으로 지원되지 않는 구성이 생성되지는 않을 경우 허용됩니다.

아래 그림과 같이 FlexPod 프로그램에는 FlexPod 익스프레스, FlexPod 데이터 센터, FlexPod 선택의 세 가지 솔루션이 포함되어 있습니다.

- * FlexPod 익스프레스 * 는 Cisco 및 NetApp의 기술을 갖춘 엔트리 레벨 솔루션을 고객에게 제공합니다.
- * FlexPod 데이터 센터 * 는 다양한 워크로드 및 애플리케이션을 위한 최적의 다목적 토대를 제공합니다.
- * FlexPod Select * 는 FlexPod 데이터 센터의 최고 기능을 통합하고 인프라를 특정 애플리케이션에 맞게 조정합니다.

다음 그림은 솔루션의 기술 구성요소를 보여 줍니다.



NetApp 검증 아키텍처 프로그램

NVA 프로그램은 NetApp 솔루션을 위한 검증된 아키텍처를 고객에게 제공합니다. NVA는 NetApp 솔루션 아키텍처의 다음과 같은 특징을 제공합니다.

- 철저한 테스트를 거친 아키텍처
- 기본적으로 규범적인 아키텍처
- 구축 위험 최소화
- 출시 시기를 단축합니다

이 가이드는 직접 연결 NetApp 스토리지를 사용하는 FlexPod Express의 설계에 대해 자세히 설명합니다. 다음 섹션에서는 이 솔루션 설계에 사용되는 구성 요소를 나열합니다.

하드웨어 구성 요소

- NetApp AFF A220을 참조하십시오
- Cisco UCS Mini를 참조하십시오
- Cisco UCS B200 M5
- Cisco UCS VIC 1440/1480.
- Cisco Nexus 3000 시리즈 스위치

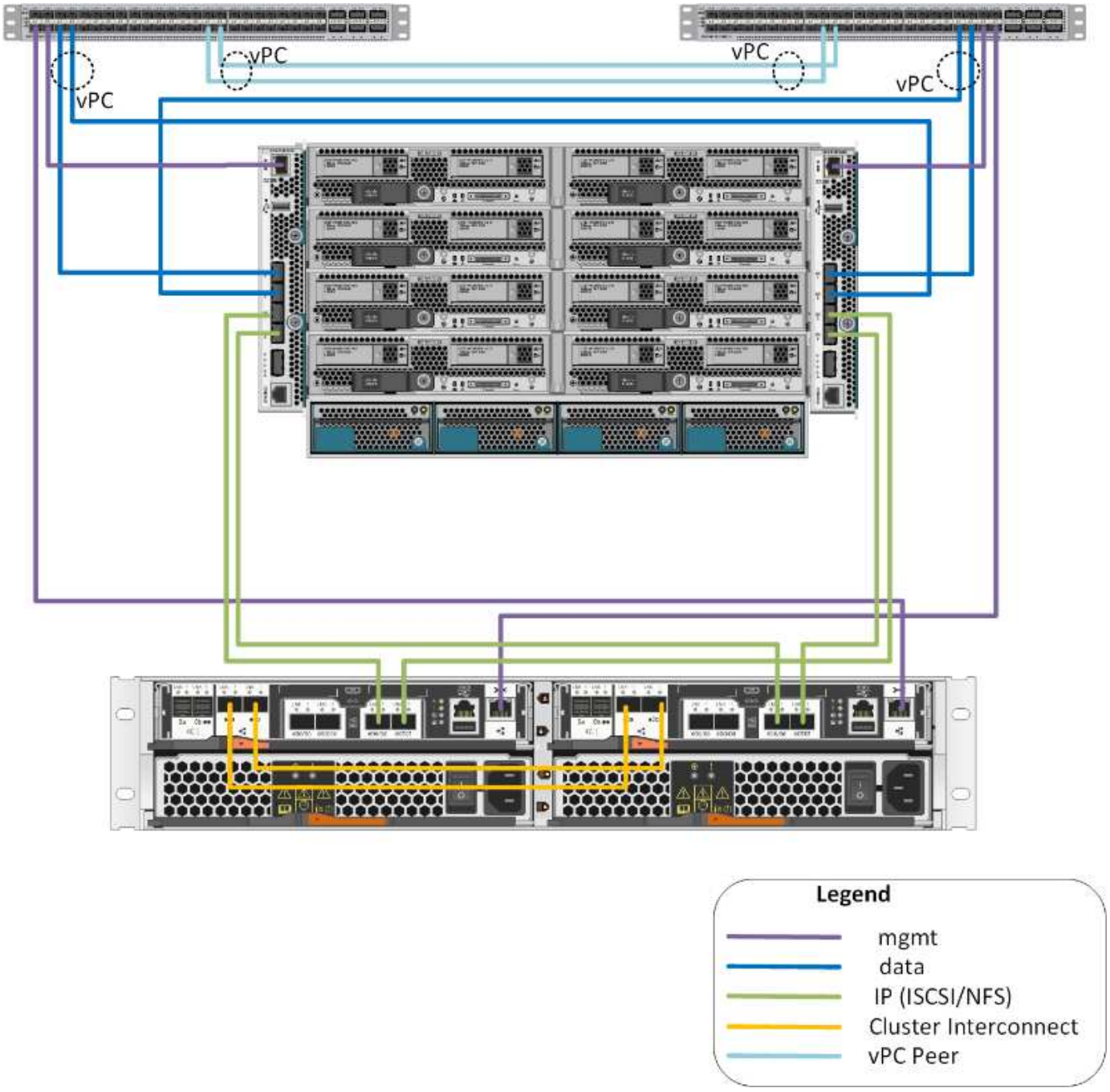
소프트웨어 구성 요소

- NetApp ONTAP 9. 5
- VMware vSphere 6.7U1
- Cisco UCS Manager 4.0(1b)
- Cisco NXOS 펌웨어 7.0(3) I6(1)

솔루션 기술

이 솔루션은 NetApp, Cisco 및 VMware의 최신 기술을 활용합니다. ONTAP 9.5, 이중 Cisco Nexus 31108PCV 스위치를 실행하는 새로운 NetApp AFF A220과 VMware vSphere 6.7U1을 실행하는 Cisco UCS B200 M5 서버를 특징으로 합니다. 이 검증된 솔루션은 10GbE 기술을 통한 Direct Connect IP 스토리지를 사용합니다.

다음 그림에서는 VMware vSphere 6.7U1 IP 기반 직접 연결 아키텍처를 지원하는 FlexPod Express를 보여 줍니다.



사용 사례 요약

FlexPod 익스프레스 솔루션은 다음과 같은 여러 사용 사례에 적용할 수 있습니다.

- ROBO
- 중소기업
- 비용 효율적인 전용 솔루션이 필요한 환경

FlexPod Express는 가상화된 혼합 워크로드에 가장 적합합니다.

기술 요구 사항

FlexPod 익스프레스 시스템에는 하드웨어 및 소프트웨어 구성 요소의 조합이 필요합니다. 또한 FlexPod Express는 하이퍼바이저 노드를 시스템에 추가하는 데 필요한 하드웨어 구성요소를 2개 단위로 설명합니다.

하드웨어 요구 사항

선택한 하이퍼바이저에 관계없이 모든 FlexPod Express 구성은 동일한 하드웨어를 사용합니다. 따라서 비즈니스 요구사항이 변경되더라도 두 하이퍼바이저 중 하나를 동일한 FlexPod Express 하드웨어에서 실행할 수 있습니다.

다음 표에는 모든 FlexPod Express 구성에 필요한 하드웨어 구성요소가 나와 있습니다.

하드웨어	수량
AFF A220 HA 쌍	1
Cisco UCS B200 M5 서버	2
Cisco Nexus 31108PCV 스위치	2
Cisco UCS B200 M5 서버용 Cisco UCS VIC(Virtual Interface Card) 1440	2
2개의 통합 UCS-Fi-M-6324 패브릭 인터커넥트를 지원하는 Cisco UCS Mini	1

소프트웨어 요구 사항

다음 표에는 FlexPod 익스프레스 솔루션의 아키텍처를 구현하는 데 필요한 소프트웨어 구성 요소가 나열되어 있습니다.

소프트웨어	버전	세부 정보
Cisco UCS Manager를 참조하십시오	4.0(1b)	Cisco UCS Fabric Interconnect Fi - 6324UP
Cisco Blade 소프트웨어	4.0(1b)	Cisco UCS B200 M5 서버용
Cisco nenic 드라이버	1.0.25.0	Cisco VIC 1440 인터페이스 카드용
Cisco NX-OS입니다	7.0(3) I6(1)	Cisco Nexus 31108PCV 스위치의 경우
NetApp ONTAP를 참조하십시오	9.5	AFF A220 컨트롤러

다음 표에는 FlexPod Express의 모든 VMware vSphere 구축에 필요한 소프트웨어가 나와 있습니다.

소프트웨어	버전
VMware vCenter Server 어플라이언스	6.7U1
VMware vSphere ESXi 하이퍼바이저	6.7U1

FlexPod 익스프레스 케이블 연결 정보

참조 검증 케이블 연결은 다음 표에 설명되어 있습니다.

다음 표에는 Cisco Nexus 스위치 31108PCV A의 케이블 연결 정보가 나열되어 있습니다

로컬 장치	로컬 포트	원격 장치	원격 포트
Cisco Nexus 스위치 31108PCV A	eth1/1	NetApp AFF A220 스토리지 컨트롤러 A입니다	e0M
	eth1/2	Cisco UCS-미니 FI-A	mgmt0
	eth1/3	Cisco UCS-미니 FI-A	eth1/1
	eth 1/4입니다	Cisco UCS-미니 FI-B를 지원합니다	eth1/1
	eth 1/13	Cisco NX 31108PCV B	eth 1/13
	eth 1/14	Cisco NX 31108PCV B	eth 1/14

다음 표에는 Cisco Nexus 스위치 31108PCV B의 케이블 연결 정보가 나와 있습니다

로컬 장치	로컬 포트	원격 장치	원격 포트
Cisco Nexus 스위치 31108PCV B	eth1/1	NetApp AFF A220 스토리지 컨트롤러 B입니다	e0M
	eth1/2	Cisco UCS-미니 FI-B를 지원합니다	mgmt0
	eth1/3	Cisco UCS-미니 FI-A	eth1/2
	eth 1/4입니다	Cisco UCS-미니 FI-B를 지원합니다	eth1/2
	eth 1/13	Cisco NX 31108PCV A	eth 1/13
	eth 1/14	Cisco NX 31108PCV A	eth 1/14

다음 표에서는 NetApp AFF A220 스토리지 컨트롤러 A의 케이블 연결 정보를 보여 줍니다

로컬 장치	로컬 포트	원격 장치	원격 포트
NetApp AFF A220 스토리지 컨트롤러 A입니다	e0a	NetApp AFF A220 스토리지 컨트롤러 B입니다	e0a
	e0b	NetApp AFF A220 스토리지 컨트롤러 B입니다	e0b
	e0e	Cisco UCS-미니 FI-A	eth1/3
	e0f	Cisco UCS-미니 FI-B를 지원합니다	eth1/3
	e0M	Cisco NX 31108PCV A	eth1/1

다음 표에서는 NetApp AFF A220 스토리지 컨트롤러 B의 케이블 연결 정보를 보여 줍니다

로컬 장치	로컬 포트	원격 장치	원격 포트
NetApp AFF A220 스토리지 컨트롤러 B입니다	e0a	NetApp AFF A220 스토리지 컨트롤러 B입니다	e0a
	e0b	NetApp AFF A220 스토리지 컨트롤러 B입니다	e0b
	e0e	Cisco UCS-미니 FI-A	eth1/4
	e0f	Cisco UCS-미니 FI-B를 지원합니다	eth1/4
	e0M	Cisco NX 31108PCV B	eth1/1

다음 표에는 Cisco UCS Fabric Interconnect A의 케이블 연결 정보가 나와 있습니다

로컬 장치	로컬 포트	원격 장치	원격 포트
Cisco UCS 6120 패브릭 인터커넥트 A	eth1/1	Cisco NX 31108PCV A	eth1/3
	eth1/2	Cisco NX 31108PCV B	eth1/3
	eth1/3	NetApp AFF A220 스토리지 컨트롤러 A입니다	e0e
	eth1/4	NetApp AFF A220 스토리지 컨트롤러 B입니다	e0e
	mgmt0	Cisco NX 31108PCV A	eth1/2

다음 표에는 Cisco UCS Fabric Interconnect B의 케이블 연결 정보가 나와 있습니다

로컬 장치	로컬 포트	원격 장치	원격 포트
Cisco UCS 6120 패브릭 인터커넥트 B	eth1/1	Cisco NX 31108PCV A	eth1/4
	eth1/2	Cisco NX 31108PCV B	eth1/4
	eth1/3	NetApp AFF A220 스토리지 컨트롤러 A입니다	e0f
	eth1/4	NetApp AFF A220 스토리지 컨트롤러 B입니다	e0f
	mgmt0	Cisco NX 31108PCV B	eth1/2

구현 절차

이 문서에서는 완전히 이중화된 고가용성 FlexPod Express 시스템을 구성하는 방법에 대해 자세히 설명합니다. 이러한 이중화를 반영하기 위해 각 단계에서 구성 요소를 구성 요소 A 또는 구성 요소 B라고 합니다 예를 들어 컨트롤러 A와 컨트롤러 B는 이 문서에 프로비저닝된 NetApp 스토리지 컨트롤러 2개를 식별합니다. 스위치 A와 스위치 B는 Cisco Nexus 스위치 쌍을 나타냅니다. 패브릭 인터커넥트 A와 패브릭 인터커넥트 B는 통합 Nexus 패브릭 인터커넥트 2개입니다.

또한 서버 A, 서버 B 등으로 순차적으로 구분되는 여러 Cisco UCS 호스트를 프로비저닝하는 단계도 설명합니다.

사용자 환경과 관련된 정보를 단계별로 포함해야 함을 나타내기 위해 명령 구조의 일부로 '<<text>>'이 표시됩니다. 'VLAN create' 명령은 다음 예를 참조하십시오.

```
Controller01>vlan create vif0 <<mgmt_vlan_id>>
```

이 문서를 사용하여 FlexPod Express 환경을 완전히 구성할 수 있습니다. 이 프로세스에서 다양한 단계를 수행하려면 고객별 명명 규칙, IP 주소 및 VLAN(Virtual Local Area Network) 스키마를 삽입해야 합니다. 아래 표에는 이 가이드에 설명된 대로 구축에 필요한 VLAN이 설명되어 있습니다. 이 표는 특정 사이트 변수를 기반으로 완료할 수 있으며 문서 구성 단계를 구현하는 데 사용할 수 있습니다.

별도의 대역내 및 대역외 관리 VLAN을 사용하는 경우 이 VLAN 사이에 계층 3 라우트를 생성해야 합니다. 이 검증에서는 공통 관리 VLAN이 사용되었습니다.

VLAN 이름입니다	**VLAN**의 용도	이 문서의 유효성을 검사하는 데 사용되는 **ID**입니다
관리 VLAN	관리 인터페이스용 VLAN	18
네이티브 VLAN	태그가 지정되지 않은 프레임이 할당되는 VLAN입니다	2
NFS VLAN	NFS 트래픽용 VLAN	104
VMware vMotion VLAN	가상 머신(VM)을 하나의 물리적 호스트에서 다른 물리적 호스트로 이동하도록 지정된 VLAN	103
VM 트래픽 VLAN	VM 애플리케이션 트래픽용 VLAN	102
iSCSI-A-VLAN	패브릭 A의 iSCSI 트래픽용 VLAN	124를 참조하십시오
iSCSI-B-VLAN	패브릭 B의 iSCSI 트래픽용 VLAN	125

FlexPod Express를 구성하는 동안 VLAN 번호가 필요합니다. VLAN은 "<<var_xxxx_vlan>>"라고 하며, 여기서 "xxxx"는 VLAN의 목적(예: iSCSI-A)입니다.

다음 표에는 생성된 VMware VM이 나와 있습니다.

VM 설명	호스트 이름
VMware vCenter Server를 참조하십시오	Seahawks-vcsa.cie.netapp.com

Cisco Nexus 31108PCV 전개 절차

이 섹션에서는 FlexPod 익스프레스 환경에서 사용되는 Cisco Nexus 31308PCV 스위치 구성에 대해 자세히 설명합니다.

Cisco Nexus 31108PCV 스위치의 초기 설정

이 절차에서는 기본 FlexPod Express 환경에서 사용할 Cisco Nexus 스위치를 구성하는 방법에 대해 설명합니다.

이 절차에서는 NX-OS 소프트웨어 릴리즈 7.0(3) I6(1)을 실행하는 Cisco Nexus 31108PCV를 사용하고 있다고 가정합니다.

1. 초기 부팅이 완료되고 스위치의 콘솔 포트에 연결되면 Cisco NX-OS 설정이 자동으로 시작됩니다. 이 초기 구성에서는 스위치 이름, mgmt0 인터페이스 구성, SSH(Secure Shell) 설정과 같은 기본 설정을 지정합니다.
2. FlexPod 익스프레스 관리 네트워크는 여러 가지 방법으로 구성할 수 있습니다. 31108PCV 스위치의 mgmt0 인터페이스를 기존 관리 네트워크에 연결하거나, 31108PCV 스위치의 mgmt0 인터페이스를 연속 구성으로 연결할 수 있습니다. 하지만 이 링크는 SSH 트래픽과 같은 외부 관리 액세스에 사용할 수 없습니다.

   이 구축 가이드에서는 FlexPod Express Cisco Nexus 31108PCV 스위치가 기존 관리 네트워크에 연결되어 있습니다.
3. Cisco Nexus 31108PCV 스위치를 구성하려면, 스위치의 전원을 켜고 화면에 표시되는 메시지에 따라 두 스위치를 초기 설정하고 스위치 관련 정보에 해당하는 값을 대체합니다.

```
This setup utility will guide you through the basic configuration of the
system. Setup configures only enough connectivity for management of the
system.
```

```
*Note: setup is mainly used for configuring the system initially, when
no configuration is present. So setup always assumes system defaults and
not the current system configuration values.
Press Enter at anytime to skip a dialog. Use ctrl-c at anytime to skip
the remaining dialogs.
Would you like to enter the basic configuration dialog (yes/no): y
Do you want to enforce secure password standard (yes/no) [y]: y
Create another login account (yes/no) [n]: n
Configure read-only SNMP community string (yes/no) [n]: n
Configure read-write SNMP community string (yes/no) [n]: n
Enter the switch name : 31108PCV-A
Continue with Out-of-band (mgmt0) management configuration? (yes/no)
[y]: y
Mgmt0 IPv4 address : <<var_switch_mgmt_ip>>
Mgmt0 IPv4 netmask : <<var_switch_mgmt_netmask>>
Configure the default gateway? (yes/no) [y]: y
IPv4 address of the default gateway : <<var_switch_mgmt_gateway>>
Configure advanced IP options? (yes/no) [n]: n
Enable the telnet service? (yes/no) [n]: n
Enable the ssh service? (yes/no) [y]: y
Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa
Number of rsa key bits <1024-2048> [1024]: <enter>
Configure the ntp server? (yes/no) [n]: y
NTP server IPv4 address : <<var_ntp_ip>>
Configure default interface layer (L3/L2) [L2]: <enter>
Configure default switchport interface state (shut/noshut) [noshut]:
<enter>
Configure CoPP system profile (strict/moderate/lenient/dense) [strict]:
<enter>
```

4. 구성 요약이 표시되고 구성을 편집할지 묻는 메시지가 표시됩니다. 구성이 올바르면 n을 입력합니다.

```
Would you like to edit the configuration? (yes/no) [n]: no
```

5. 그런 다음 이 구성을 사용하고 저장할지 묻는 메시지가 표시됩니다. 그렇다면 y를 입력합니다.

```
Use this configuration and save it? (yes/no) [y]: Enter
```

6. Cisco Nexus 스위치 B에 대해 1단계부터 5단계까지 반복합니다

고급 기능을 활성화합니다

추가 구성 옵션을 제공하려면 Cisco NX-OS에서 특정 고급 기능을 사용하도록 설정해야 합니다.

1. Cisco Nexus 스위치 A와 스위치 B에서 적절한 기능을 활성화하려면 '(config t)' 명령을 사용하여 구성 모드를 시작하고 다음 명령을 실행합니다.

```
feature interface-vlan
feature lacp
feature vpc
```

> 기본 포트 채널 로드 밸런싱 해쉬는 소스 및 타깃 IP 주소를 사용하여 포트 채널의 인터페이스에 대한 로드 밸런싱 알고리즘을 결정합니다. 소스 및 타깃 IP 주소보다 많은 입력을 해쉬 알고리즘에 제공하면 포트 채널 멤버 전체에 걸쳐 더 효율적으로 분산될 수 있습니다. 동일한 이유로 소스 및 타깃 TCP 포트를 해쉬 알고리즘에 추가하는 것이 좋습니다.

2. 구성 모드 '(config t)에서 다음 명령을 실행하여 Cisco Nexus 스위치 A 및 스위치 B의 글로벌 포트 채널 로드 밸런싱 구성을 설정하십시오.

```
port-channel load-balance src-dst ip-l4port
```

글로벌 스패닝 트리 구성을 수행합니다

Cisco Nexus 플랫폼은 브리지 보장이라는 새로운 보호 기능을 사용합니다. 브리지 보장은 스패닝 트리 알고리즘을 더 이상 실행하지 않는 장치에서 데이터 트래픽을 계속 전달하는 단방향 링크 또는 기타 소프트웨어 장애를 방지합니다. 플랫폼에 따라 네트워크 또는 가장자리를 포함한 여러 상태 중 하나에 포트를 배치할 수 있습니다.

기본적으로 모든 포트가 네트워크 포트로 간주되도록 브리지 보장을 설정하는 것이 좋습니다. 이 설정은 네트워크 관리자가 각 포트의 구성을 검토하도록 합니다. 또한 확인되지 않은 에지 포트 또는 브리지 보장 기능이 활성화되지 않은 인접 장치와 같은 가장 일반적인 구성 오류도 표시됩니다. 또한 스패닝 트리에서 너무 적은 포트가 아니라 많은 포트를 차단하는 편이 더 안전합니다. 그러면 기본 포트 상태를 통해 네트워크의 전반적인 안정성을 향상할 수 있습니다.

특히 브리지 보장을 지원하지 않는 서버, 스토리지 및 업링크 스위치를 추가할 때는 스패닝 트리 상태에 세심한 주의를 기울여야 합니다. 이러한 경우 포트를 활성화하려면 포트 유형을 변경해야 할 수 있습니다.

브리지 프로토콜 데이터 단위(BPDU) 보호대는 기본적으로 다른 보호 계층으로 에지 포트에서 활성화됩니다. 네트워크의 루프를 방지하기 위해 이 기능은 다른 스위치의 BPDU가 이 인터페이스에 표시되는 경우 포트를 종료합니다.

구성 모드('config t')에서 다음 명령을 실행하여 Cisco Nexus 스위치 A 및 스위치 B에서 기본 포트 유형과 BPDU 가드를 포함한 기본 스패닝 트리 옵션을 구성하십시오.

```
spanning-tree port type network default
spanning-tree port type edge bpduguard default
```

VLAN을 정의합니다

VLAN이 서로 다른 개별 포트를 구성하기 전에 스위치에서 레이어 2 VLAN을 정의해야 합니다. 향후 문제 해결이 용이하도록 VLAN 이름을 지정하는 것도 좋은 방법입니다.

구성 모드('config t')에서 다음 명령을 실행하여 Cisco Nexus 스위치 A 및 스위치 B의 계층 2 VLAN을 정의하고 설명하십시오.

```
vlan <<nfs_vlan_id>>
  name NFS-VLAN
vlan <<iSCSI_A_vlan_id>>
  name iSCSI-A-VLAN
vlan <<iSCSI_B_vlan_id>>
  name iSCSI-B-VLAN
vlan <<vmotion_vlan_id>>
  name vMotion-VLAN
vlan <<vmtraffic_vlan_id>>
  name VM-Traffic-VLAN
vlan <<mgmt_vlan_id>>
  name MGMT-VLAN
vlan <<native_vlan_id>>
  name NATIVE-VLAN
exit
```

액세스 및 관리 포트 설명을 구성합니다

레이어 2 VLAN에 이름을 할당하는 경우와 마찬가지로, 모든 인터페이스에 대한 설정 설명은 프로비저닝과 문제 해결에 도움이 될 수 있습니다.

각 스위치의 구성 모드('config t')에서 FlexPod Express 대규모 구성에 대한 다음 포트 설명을 입력합니다.

Cisco Nexus 스위치 **A**

```
int eth1/1
  description AFF A220-A e0M
int eth1/2
  description Cisco UCS FI-A mgmt0
int eth1/3
  description Cisco UCS FI-A eth1/1
int eth1/4
  description Cisco UCS FI-B eth1/1
int eth1/13
  description vPC peer-link 31108PVC-B 1/13
int eth1/14
  description vPC peer-link 31108PVC-B 1/14
```

Cisco Nexus 스위치 **B**

```
int eth1/1
  description AFF A220-B e0M
int eth1/2
  description Cisco UCS FI-B mgmt0
int eth1/3
  description Cisco UCS FI-A eth1/2
int eth1/4
  description Cisco UCS FI-B eth1/2
int eth1/13
  description vPC peer-link 31108PVC-B 1/13
int eth1/14
  description vPC peer-link 31108PVC-B 1/14
```

서버 및 스토리지 관리 인터페이스를 구성합니다

서버와 스토리지 모두의 관리 인터페이스는 일반적으로 단일 VLAN만 사용합니다. 따라서 관리 인터페이스 포트를 액세스 포트로 구성합니다. 각 스위치에 대한 관리 VLAN을 정의하고 스패닝 트리 포트 유형을 에지로 변경합니다.

구성 모드('config t')에서 다음 명령을 실행하여 서버와 스토리지 모두의 관리 인터페이스에 대한 포트 설정을 구성하십시오.

Cisco Nexus 스위치 **A**

```
int eth1/1-2
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

Cisco Nexus 스위치 **B**

```
int eth1/1-2
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

NTP 배포 인터페이스를 추가합니다

Cisco Nexus 스위치 **A**

글로벌 구성 모드에서 다음 명령을 실행합니다.

```
interface Vlan<ib-mgmt-vlan-id>
ip address <switch-a-ntp-ip>/<ib-mgmt-vlan-netmask-length>
no shutdown
exitntp peer <switch-b-ntp-ip> use-vrf default
```

Cisco Nexus 스위치 **B**

글로벌 구성 모드에서 다음 명령을 실행합니다.

```
interface Vlan<ib-mgmt-vlan-id>
ip address <switch- b-ntp-ip>/<ib-mgmt-vlan-netmask-length>
no shutdown
exitntp peer <switch-a-ntp-ip> use-vrf default
```

가상 포트 채널 글로벌 구성을 수행합니다

가상 포트 채널(vPC)을 사용하면 물리적으로 두 개의 서로 다른 Cisco Nexus 스위치에 연결된 링크가 세 번째 장치에 단일 포트 채널로 표시될 수 있습니다. 세 번째 장치는 스위치, 서버 또는 다른 네트워킹 장치일 수 있습니다. vPC는 계층 2 다중 경로를 제공할 수 있으므로 대역폭을 높이고, 노드 간에 여러 개의 병렬 경로를 활성화하고, 대체 경로가 있는 로드 밸런싱 트래픽을 통해 이중화를 생성할 수 있습니다.

vPC는 다음과 같은 이점을 제공합니다.

- 단일 장치에서 두 업스트림 장치에 걸쳐 포트 채널을 사용하도록 설정
- 스패닝 트리 프로토콜 차단 포트 제거
- 루프 없는 토폴로지 제공
- 사용 가능한 모든 업링크 대역폭 사용
- 링크 또는 디바이스에 장애가 발생할 경우 빠른 컨버전스를 제공합니다
- 링크 레벨의 복원력 제공
- 고가용성 제공 지원

vPC 기능이 제대로 작동하려면 두 Cisco Nexus 스위치 간의 몇 가지 초기 설정이 필요합니다. 연속 인접 mgmt0 구성을 사용하는 경우에는 인터페이스에 정의된 주소를 사용하고 ping "<<switch_a/B_mgmt0_ip_addr>>VRF" 관리 명령을 사용하여 통신 가능 여부를 확인해야 합니다.

구성 모드('config t')에서 다음 명령을 실행하여 두 스위치에 대한 vPC 글로벌 구성을 설정하십시오.

Cisco Nexus 스위치 **A**

```
vpc domain 1
 role priority 10
peer-keepalive destination <<switch_B_mgmt0_ip_addr>> source
<<switch_A_mgmt0_ip_addr>> vrf management
  peer-gateway
  auto-recovery
  ip arp synchronize
  int eth1/13-14
  channel-group 10 mode active
int Po10description vPC peer-link
switchport
switchport mode trunkswitchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>> spanning-tree port type network
vpc peer-link
no shut
exit
int Po13
description vPC ucs-FI-A
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<vmotion_vlan_id>>, <<vmtraffic_vlan_id>>,
<<mgmt_vlan>> spanning-tree port type network
mtu 9216
vpc 13
no shut
exit
int eth1/3
  channel-group 13 mode active
int Po14
description vPC ucs-FI-B
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<vmotion_vlan_id>>, <<vmtraffic_vlan_id>>,
<<mgmt_vlan>> spanning-tree port type network
mtu 9216
vpc 14
no shut
exit
int eth1/4
  channel-group 14 mode active
copy run start
```

Cisco Nexus 스위치 B

```
vpc domain 1
peer-switch
role priority 20
peer-keepalive destination <<switch_A_mgmt0_ip_addr>> source
<<switch_B_mgmt0_ip_addr>> vrf management
  peer-gateway
  auto-recovery
  ip arp synchronize
  int eth1/13-14
  channel-group 10 mode active
int Po10
description vPC peer-link
switchport
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>> spanning-tree port type network
vpc peer-link
no shut
exit
int Po13
description vPC ucs-FI-A
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<vmotion_vlan_id>>, <<vmtraffic_vlan_id>>,
<<mgmt_vlan>> spanning-tree port type network
mtu 9216
vpc 13
no shut
exit
int eth1/3
  channel-group 13 mode active
int Po14
description vPC ucs-FI-B
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<vmotion_vlan_id>>, <<vmtraffic_vlan_id>>,
<<mgmt_vlan>> spanning-tree port type network
mtu 9216
vpc 14
no shut
exit
int eth1/4
```

```
  channel-group 14 mode active
copy run start
```

이 솔루션 검증에서 MTU(Maximum Transmission Unit) 9000이 사용되었습니다. 그러나 애플리케이션 요구 사항에 따라 MTU의 적절한 값을 구성할 수 있습니다. FlexPod 솔루션에서 동일한 MTU 값을 설정하는 것이 중요합니다. 구성 요소 간의 MTU 구성이 잘못되면 패킷이 삭제됩니다.

기존 네트워크 인프라로 업링크

사용 가능한 네트워크 인프라에 따라 여러 가지 방법과 기능을 사용하여 FlexPod 환경을 업링크할 수 있습니다. 기존 Cisco Nexus 환경이 존재하는 경우, NetApp은 vPC를 사용하여 FlexPod 환경에 포함된 Cisco Nexus 31108PVC 스위치를 인프라로 업링크하는 것을 권장합니다. 업링크는 10GbE 인프라스트럭처 솔루션의 경우 10GbE 업링크, 필요한 경우 1GbE 인프라스트럭처 솔루션의 경우 1GbE가 될 수 있습니다. 앞서 설명한 절차를 사용하여 기존 환경에 대한 업링크 vPC를 생성할 수 있습니다. 구성이 완료된 후 각 스위치에 대한 구성을 저장하려면 copy run start를 실행해야 합니다.

NetApp 스토리지 구축 절차(1부)

이 섹션에서는 NetApp AFF 스토리지 구축 절차를 설명합니다.

NetApp 스토리지 컨트롤러 AFF2xx 시리즈 설치

NetApp Hardware Universe를 참조하십시오

를 클릭합니다 "NetApp Hardware Universe를 참조하십시오" (HWU) 애플리케이션은 특정 ONTAP 버전에 대해 지원되는 하드웨어 및 소프트웨어 구성요소를 제공합니다. 현재 ONTAP 소프트웨어가 지원하는 모든 NetApp 스토리지 어플라이언스에 대한 구성 정보를 제공합니다. 구성요소 호환성 표도 제공합니다.

사용하려는 하드웨어 및 소프트웨어 구성 요소가 설치하려는 ONTAP 버전에서 지원되는지 확인합니다.

1. 에 액세스합니다 "HWU" 응용 프로그램 - 시스템 구성 가이드를 봅니다. 스토리지 시스템 비교 탭을 선택하여 ONTAP 소프트웨어의 다른 버전과 원하는 사양이 있는 NetApp 스토리지 어플라이언스 간의 호환성을 확인하십시오.
2. 또는 스토리지 어플라이언스별로 구성 요소를 비교하려면 스토리지 시스템 비교 를 클릭합니다.

컨트롤러 AFF2XX 시리즈 사전 요구 사항
스토리지 시스템의 물리적 위치를 계획하려면 다음 섹션을 참조하십시오. 전기 요구 사항 지원되는 전원 코드 온보드 포트 및 케이블

스토리지 컨트롤러

의 컨트롤러에 대한 물리적 설치 절차를 따릅니다 "AFF A220 문서".

NetApp ONTAP 9.5

구성 워크시트

설치 스크립트를 실행하기 전에 제품 설명서에서 구성 워크시트를 작성하십시오. 구성 워크시트는 에서 사용할 수 있습니다 "ONTAP 9.5 소프트웨어 설치 안내서" (에서 사용 가능 "ONTAP 9 문서 센터")를 클릭합니다. 아래 표에는 ONTAP 9.5 설치 및 구성 정보가 나와 있습니다.

이 시스템은 스위치가 없는 2노드 클러스터 구성에서 설정됩니다.

클러스터 세부 정보	클러스터 세부 정보 값입니다
클러스터 노드 A IP 주소입니다	<<var_NodeA_mgmt_ip>> 를 입력합니다
클러스터 노드 A 넷마스크	<<var_NodeA_mgmt_mask>> 를 입력합니다
클러스터 노드 A 게이트웨이	<<var_NodeA_mgmt_gateway>> 를 참조하십시오
클러스터 노드 A 이름	<<var_NodeA>> 를 참조하십시오
클러스터 노드 B IP 주소입니다	<<var_NodeB_mgmt_ip>> 를 입력합니다
클러스터 노드 B 넷마스크	<<var_NodeB_mgmt_mask>> 를 입력합니다
클러스터 노드 B 게이트웨이	<<var_NodeB_mgmt_gateway>> 를 참조하십시오
클러스터 노드 B 이름	<<var_NodeB>> 를 참조하십시오
ONTAP 9.5 URL	<<var_url_boot_software>>
클러스터의 이름입니다	<<var_clustername>> 를 클릭합니다
클러스터 관리 IP 주소입니다	<<var_clustermgmt_ip>> 를 입력합니다
클러스터 B 게이트웨이	<<var_clustermgmt_gateway>> 를 클릭합니다
클러스터 B 넷마스크	<<var_clustermgmt_mask>> 를 입력합니다
도메인 이름	<<var_domain_name>>
DNS 서버 IP(둘 이상 입력할 수 있음)	<<var_dns_server_ip>> 를 참조하십시오
NTP 서버 A IP입니다	스위치-A-NTP-IP>>
NTP 서버 B IP입니다	switch-b-ntp-ip>>

노드 **A**를 구성합니다

노드 A를 구성하려면 다음 단계를 완료하십시오.

1. 스토리지 시스템 콘솔 포트에 연결합니다. Loader-A 메시지가 표시됩니다. 하지만 스토리지 시스템이 재부팅 루프 상태인 경우 다음 메시지가 표시될 때 Ctrl-C를 눌러 자동 부팅 루프를 종료합니다.

```
Starting AUTOBOOT press Ctrl-C to abort...
```

2. 시스템이 부팅되도록 합니다.

```
autoboot
```

3. Ctrl-C를 눌러 부팅 메뉴로 들어갑니다.

   ONTAP 9인 경우 5는 부팅 중인 소프트웨어 버전이 아닙니다. 새 소프트웨어를 설치하려면 다음 단계를 계속 수행하십시오. ONTAP 9인 경우 5는 부팅 중인 버전이며 옵션 8과 y를 선택하여 노드를 재부팅합니다. 그런 다음 14단계를 계속합니다.

4. 새 소프트웨어를 설치하려면 옵션 '7'을 선택합니다.
5. 업그레이드를 수행하려면 y를 입력하십시오.
6. 다운로드에 사용할 네트워크 포트로 e0M 을 선택합니다.
7. 지금 재부팅하려면 y를 입력하십시오.
8. 각 위치에 e0M의 IP 주소, 넷마스크 및 기본 게이트웨이를 입력합니다.

```
<<var_nodeA_mgmt_ip>> <<var_nodeA_mgmt_mask>> <<var_nodeA_mgmt_gateway>>
```

9. 소프트웨어를 찾을 수 있는 URL을 입력합니다.

   이 웹 서버는 Ping할 수 있어야 합니다.

10. 사용자 이름에 대해 Enter 키를 눌러 사용자 이름이 없음을 나타냅니다.
11. 새로 설치한 소프트웨어를 이후 재부팅에 사용할 기본값으로 설정하려면 'y'를 입력합니다.
12. 노드를 재부팅하려면 y를 입력합니다.

    새 소프트웨어를 설치할 때 시스템이 BIOS 및 어댑터 카드에 대한 펌웨어 업그레이드를 수행할 수 있으며, 이로 인해 LOADER-A 프롬프트에서 재부팅되고 중지될 수 있습니다. 이러한 작업이 발생하면 시스템이 이 절차를 벗어날 수 있습니다.

13. Ctrl-C를 눌러 부팅 메뉴로 들어갑니다.
14. Clean Configuration 및 Initialize All Disks 옵션을 4로 선택합니다.
15. 디스크를 제로화하려면 y를 입력하고 구성을 재설정한 다음 새 파일 시스템을 설치합니다.
16. 디스크에 있는 모든 데이터를 지우려면 'y'를 입력합니다.

    연결된 디스크의 수와 유형에 따라 루트 애그리게이트의 초기화 및 생성을 완료하는 데 90분 이상이 걸릴 수 있습니다. 초기화가 완료되면 스토리지 시스템이 재부팅됩니다. SSD를 초기화하는 데 걸리는 시간은 상당히 줄어듭니다. 노드 A용 디스크가 제로화하는 동안 노드 B 구성을 계속할 수 있습니다.

17. 노드 A를 초기화하는 동안 노드 B를 구성합니다

노드 **B**를 구성합니다

노드 B를 구성하려면 다음 단계를 완료하십시오.

1. 스토리지 시스템 콘솔 포트에 연결합니다. Loader-A 메시지가 표시됩니다. 하지만 스토리지 시스템이 재부팅 루프 상태인 경우 다음 메시지가 표시될 때 Ctrl-C를 눌러 자동 부팅 루프를 종료합니다.

```
Starting AUTOBOOT press Ctrl-C to abort...
```

2. Ctrl-C를 눌러 부팅 메뉴로 들어갑니다.

```
autoboot
```

3. 메시지가 나타나면 Ctrl-C를 누릅니다.

   ONTAP 9인 경우 5는 부팅 중인 소프트웨어 버전이 아닙니다. 새 소프트웨어를 설치하려면 다음 단계를 계속 수행하십시오. ONTAP 9.4가 부팅 중인 버전인 경우 옵션 8 및 y를 선택하여 노드를 재부팅합니다. 그런 다음 14단계를 계속합니다.

4. 새 소프트웨어를 설치하려면 옵션 7을 선택합니다.
5. 업그레이드를 수행하려면 y를 입력하십시오.
6. 다운로드에 사용할 네트워크 포트로 e0M 을 선택합니다.
7. 지금 재부팅하려면 y를 입력하십시오.
8. 각 위치에 e0M의 IP 주소, 넷마스크 및 기본 게이트웨이를 입력합니다.

```
<<var_nodeB_mgmt_ip>> <<var_nodeB_mgmt_ip>><<var_nodeB_mgmt_gateway>>
```

9. 소프트웨어를 찾을 수 있는 URL을 입력합니다.

   이 웹 서버는 Ping할 수 있어야 합니다.

```
<<var_url_boot_software>>
```

10. 사용자 이름에 대해 Enter 키를 눌러 사용자 이름이 없음을 나타냅니다
11. 새로 설치한 소프트웨어를 이후 재부팅에 사용할 기본값으로 설정하려면 'y'를 입력합니다.
12. 노드를 재부팅하려면 y를 입력합니다.

    새 소프트웨어를 설치할 때 시스템이 BIOS 및 어댑터 카드에 대한 펌웨어 업그레이드를 수행할 수 있으며, 이로 인해 LOADER-A 프롬프트에서 재부팅되고 중지될 수 있습니다. 이러한 작업이 발생하면 시스템이 이 절차를 벗어날 수 있습니다.

13. Ctrl-C를 눌러 부팅 메뉴로 들어갑니다.
14. Clean Configuration(구성 정리) 및 Initialize All Disks(모든 디스크 초기화) 에 대해 옵션 4 를 선택합니다.
15. 디스크를 제로화하려면 y를 입력하고 구성을 재설정한 다음 새 파일 시스템을 설치합니다.
16. 디스크에 있는 모든 데이터를 지우려면 'y'를 입력합니다.

    연결된 디스크의 수와 유형에 따라 루트 애그리게이트의 초기화 및 생성을 완료하는 데 90분 이상이 걸릴 수 있습니다. 초기화가 완료되면 스토리지 시스템이 재부팅됩니다. SSD를 초기화하는 데 걸리는 시간은 상당히 줄어듭니다.

연속 노드 구성 및 클러스터 구성

스토리지 컨트롤러 A(노드 A) 콘솔 포트에 연결된 콘솔 포트 프로그램에서 노드 설정 스크립트를 실행합니다. 이

스크립트는 ONTAP 9.5가 노드에서 처음 부팅될 때 나타납니다.

ONTAP 9.5에서 노드 및 클러스터 설정 절차가 약간 변경되었습니다. 이제 클러스터 설정 마법사를 사용하여 클러스터의 첫 번째 노드를 구성하고 System Manager를 사용하여 클러스터를 구성할 수 있습니다.

1. 프롬프트에 따라 노드 A를 설정합니다

```
Welcome to the cluster setup wizard.
You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the cluster setup wizard.
     Any changes you made before quitting will be saved.
You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value.
This system will send event messages and periodic reports to NetApp
Technical Support. To disable this feature, enter
autosupport modify -support disable
within 24 hours.
Enabling AutoSupport can significantly speed problem determination and
resolution should a problem occur on your system.
For further information on AutoSupport, see:
http://support.netapp.com/autosupport/
Type yes to confirm and continue {yes}: yes
Enter the node management interface port [e0M]:
Enter the node management interface IP address: <<var_nodeA_mgmt_ip>>
Enter the node management interface netmask: <<var_nodeA_mgmt_mask>>
Enter the node management interface default gateway:
<<var_nodeA_mgmt_gateway>>
A node management interface on port e0M with IP address
<<var_nodeA_mgmt_ip>> has been created.
Use your web browser to complete cluster setup by accessing
https://<<var_nodeA_mgmt_ip>>
Otherwise, press Enter to complete cluster setup using the command line
interface:
```

2. 노드의 관리 인터페이스의 IP 주소로 이동합니다.

CLI를 사용하여 클러스터를 설정할 수도 있습니다. 이 문서에서는 NetApp System Manager의 안내에 따라 설정을 사용하는 클러스터 설정에 대해 설명합니다.

3. Guided Setup(안내식 설정) 을 클릭하여 클러스터를 구성합니다.
4. 클러스터 이름은 <<var_clustername>>'을, 구성 중인 각 노드에 대해서는 <<var_NodeA>>'와 <<var_NodeB>>를 입력합니다. 스토리지 시스템에 사용할 암호를 입력합니다. 클러스터 유형으로 Switchless Cluster를 선택합니다. 클러스터 기본 라이센스를 입력합니다.
5. 클러스터, NFS 및 iSCSI에 대한 기능 라이센스도 입력할 수 있습니다.

6. 클러스터를 생성 중임을 나타내는 상태 메시지가 표시됩니다. 이 상태 메시지는 여러 상태를 순환합니다. 이 과정은 몇 분 정도 소요됩니다.
7. 네트워크를 구성합니다.
   a. IP 주소 범위 옵션을 선택 취소합니다.
   b. Cluster Management IP Address 필드(<<var_clustermgmt_ip>>)에 넷마스크 필드(<<var_clustermgmt_mask>>)에 <<var_clustermgmt_gateway>>)를 입력합니다. 포트 필드의… 선택기를 사용하여 노드 A의 e0M을 선택합니다
   c. 노드 A의 노드 관리 IP가 이미 채워져 있습니다. 노드 B에 대해 '<<var_NodeA_mgmt_ip>>'를 입력합니다
   d. DNS Domain Name 필드에 '<<var_domain_name>>'을 입력합니다. DNS 서버 IP 주소 필드에 '<<var_dns_server_ip>>'를 입력합니다.

      여러 DNS 서버 IP 주소를 입력할 수 있습니다.

   e. Primary NTP Server 필드에 '<<switch-a-ntp-ip>>'를 입력합니다.

      대체 NTP 서버를 "<<switch-b-ntp-ip>>"로 입력할 수도 있습니다.
8. 지원 정보를 구성합니다.
   a. 환경에 AutoSupport에 액세스하기 위한 프록시가 필요한 경우 프록시 URL에 URL을 입력합니다.
   b. 이벤트 알림에 대한 SMTP 메일 호스트 및 이메일 주소를 입력합니다.

      계속하려면 이벤트 알림 방법을 설정해야 합니다. 방법 중 하나를 선택할 수 있습니다.
9. 클러스터 구성이 완료되었으면 클러스터 관리 를 클릭하여 스토리지를 구성합니다.

스토리지 클러스터 구성의 연속

스토리지 노드 및 기본 클러스터를 구성한 후에는 스토리지 클러스터 구성을 계속할 수 있습니다.

모든 스페어 디스크를 제로합니다

클러스터의 모든 스페어 디스크를 제로하려면 다음 명령을 실행합니다.

```
disk zerospares
```

온보드 **UTA2** 포트 속성을 설정합니다

1. ucadmin show 명령을 실행하여 현재 모드와 포트의 현재 유형을 확인합니다.

```
AFFA220-Clus::> ucadmin show
                      Current  Current    Pending  Pending    Admin
Node          Adapter  Mode     Type       Mode     Type       Status
------------  -------  -------  ---------  -------  ---------
-----------
AFFA220-Clus-01
              0c       cna      target     -        -          offline
AFFA220-Clus-01
              0d       cna      target     -        -          offline
AFFA220-Clus-01
              0e       cna      target     -        -          offline
AFFA220-Clus-01
              0f       cna      target     -        -          offline
AFFA220-Clus-02
              0c       cna      target     -        -          offline
AFFA220-Clus-02
              0d       cna      target     -        -          offline
AFFA220-Clus-02
              0e       cna      target     -        -          offline
AFFA220-Clus-02
              0f       cna      target     -        -          offline
8 entries were displayed.
```

2. 사용 중인 포트의 현재 모드가 CNA인지, 현재 유형이 'target'으로 설정되어 있는지 확인합니다. 그렇지 않은 경우 다음 명령을 실행하여 포트 속성을 변경합니다.

```
ucadmin modify -node <home node of the port> -adapter <port name> -mode
cna -type target
```

이전 명령을 실행하려면 포트가 오프라인 상태여야 합니다. 포트를 오프라인으로 전환하려면 다음 명령을 실행합니다.

```
network fcp adapter modify -node <home node of the port> -adapter <port
name> -state down
```

포트 속성을 변경한 경우 변경 사항을 적용하려면 각 노드를 재부팅해야 합니다.

Cisco Discovery Protocol을 활성화합니다

NetApp 스토리지 컨트롤러에서 CDP(Cisco Discovery Protocol)를 활성화하려면 다음 명령을 실행합니다.

```
node run -node * options cdpd.enable on
```

모든 이더넷 포트에서 링크 계층 검색 프로토콜을 활성화합니다

다음 명령을 실행하여 스토리지와 네트워크 스위치 간에 LLDP(Link-layer Discovery Protocol) 인접 정보 교환을 활성화합니다. 이 명령을 실행하면 클러스터에 있는 모든 노드의 모든 포트에 LLDP가 설정됩니다.

```
node run * options lldp.enable on
```

관리 논리 인터페이스의 이름을 바꿉니다

관리 논리 인터페이스(LIF)의 이름을 변경하려면 다음 단계를 수행하십시오.

1. 현재 관리 LIF 이름을 표시합니다.

   ```
   network interface show –vserver <<clustername>>
   ```

2. 클러스터 관리 LIF의 이름을 바꿉니다.

   ```
   network interface rename –vserver <<clustername>> –lif
   cluster_setup_cluster_mgmt_lif_1 –newname cluster_mgmt
   ```

3. 노드 B 관리 LIF의 이름을 바꿉니다.

   ```
   network interface rename -vserver <<clustername>> -lif
   cluster_setup_node_mgmt_lif_AFF A220_A_1 - newname AFF A220-01_mgmt1
   ```

클러스터 관리에서 자동 되돌리기 설정

클러스터 관리 인터페이스에서 자동 되돌리기 매개 변수를 설정합니다.

```
network interface modify –vserver <<clustername>> -lif cluster_mgmt –auto-
revert true
```

서비스 프로세서 네트워크 인터페이스를 설정합니다

각 노드의 서비스 프로세서에 정적 IPv4 주소를 할당하려면 다음 명령을 실행합니다.

```
system service-processor network modify -node <<var_nodeA>> -address
-family IPv4 -enable true - dhcp none -ip-address <<var_nodeA_sp_ip>>
-netmask <<var_nodeA_sp_mask>> -gateway <<var_nodeA_sp_gateway>>
system service-processor network modify -node <<var_nodeB>> -address
-family IPv4 -enable true - dhcp none -ip-address <<var_nodeB_sp_ip>>
-netmask <<var_nodeB_sp_mask>> -gateway <<var_nodeB_sp_gateway>>
```

서비스 프로세서 IP 주소는 노드 관리 IP 주소와 동일한 서브넷에 있어야 합니다.

ONTAP에서 스토리지 페일오버 설정

스토리지 페일오버가 설정되었는지 확인하려면 페일오버 쌍에서 다음 명령을 실행합니다.

1. 스토리지 페일오버 상태를 확인합니다.

   ```
   storage failover show
   ```

   '<<var_NodeA>>'와 '<<var_NodeB>>'는 모두 테이크오버를 수행할 수 있어야 합니다. 노드가 테이크오버 수행 가능한 경우 3단계로 이동하십시오.

2. 두 노드 중 하나에서 페일오버가 사용되도록 설정합니다.

   ```
   storage failover modify -node <<var_nodeA>> -enabled true
   ```

3. 2노드 클러스터의 HA 상태를 확인합니다.

   2개 이상의 노드가 있는 클러스터에는 이 단계를 적용할 수 없습니다.

   ```
   cluster ha show
   ```

4. 고가용성이 구성된 경우 6단계로 이동합니다. 고가용성이 구성된 경우 명령을 실행하면 다음 메시지가 표시됩니다.

   ```
   High Availability Configured: true
   ```

5. 2노드 클러스터에만 HA 모드를 사용하도록 설정합니다.

   2개 이상의 노드가 있는 클러스터에서는 페일오버에 문제가 발생하므로 이 명령을 실행하지 마십시오.

   ```
   cluster ha modify -configured true
   Do you want to continue? {y|n}: y
   ```

6. 하드웨어 지원이 올바르게 구성되어 있는지 확인하고 필요한 경우 파트너 IP 주소를 수정합니다.

```
storage failover hwassist show
```

"Keep Alive Status: Error: whwassist keep alive alert from partner(활성 상태 유지: 오류: 파트너의 hwassist keep alive 경고를 수신하지 못했습니다)" 메시지는 하드웨어 지원이 구성되지 않았음을 나타냅니다. 다음 명령을 실행하여 하드웨어 지원을 구성합니다.

```
storage failover modify –hwassist-partner-ip <<var_nodeB_mgmt_ip>> -node
<<var_nodeA>>
storage failover modify –hwassist-partner-ip <<var_nodeA_mgmt_ip>> -node
<<var_nodeB>>
```

ONTAP에서 점보 프레임 **MTU** 브로드캐스트 도메인을 생성합니다

MTU가 9000인 데이터 브로드캐스트 도메인을 생성하려면 다음 명령을 실행합니다.

```
broadcast-domain create -broadcast-domain Infra_NFS -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-A -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-B -mtu 9000
```

기본 브로드캐스트 도메인에서 데이터 포트를 제거합니다

10GbE 데이터 포트는 iSCSI/NFS 트래픽에 사용되며 이러한 포트는 기본 도메인에서 제거해야 합니다. 포트 e0e 및 e0f는 사용되지 않으며 기본 도메인에서도 제거해야 합니다.

브로드캐스트 도메인에서 포트를 제거하려면 다음 명령을 실행합니다.

```
broadcast-domain remove-ports -broadcast-domain Default -ports
<<var_nodeA>>:e0c, <<var_nodeA>>:e0d, <<var_nodeA>>:e0e,
<<var_nodeA>>:e0f, <<var_nodeB>>:e0c, <<var_nodeB>>:e0d,
<<var_nodeA>>:e0e, <<var_nodeA>>:e0f
```

UTA2 포트에서 흐름 제어를 사용하지 않도록 설정합니다

외부 장치에 연결된 모든 UTA2 포트에서 흐름 제어를 사용하지 않도록 설정하는 것이 NetApp의 모범 사례입니다. 흐름 제어를 사용하지 않도록 설정하려면 다음 명령을 실행합니다.

```
net port modify -node <<var_nodeA>> -port e0c -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0d -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0e -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0f -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0c -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0d -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0e -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0f -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
```

ONTAP에 대한 Cisco UCS Mini 직접 연결은 LACP를 지원하지 않습니다.

NetApp ONTAP에서 점보 프레임을 구성합니다

ONTAP 네트워크 포트에서 점보 프레임(일반적으로 9,000바이트 MTU 사용)을 사용하도록 구성하려면 클러스터 쉘에서 다음 명령을 실행합니다.

```
AFF A220::> network port modify -node node_A -port e0e -mtu 9000
Warning: This command will cause a several second interruption of service
on this network port.
Do you want to continue? {y|n}: y
AFF A220::> network port modify -node node_B -port e0e -mtu 9000
Warning: This command will cause a several second interruption of service
on this network port.
Do you want to continue? {y|n}: y
AFF A220::> network port modify -node node_A -port e0f -mtu 9000
Warning: This command will cause a several second interruption of service
on this network port.
Do you want to continue? {y|n}: y
AFF A220::> network port modify -node node_B -port e0f -mtu 9000
Warning: This command will cause a several second interruption of service
on this network port.
Do you want to continue? {y|n}: y
```

ONTAP에서 **VLAN**을 생성합니다

ONTAP에서 VLAN을 생성하려면 다음 단계를 수행하십시오.

1. NFS VLAN 포트를 생성하여 데이터 브로드캐스트 도메인에 추가합니다.

```
network port vlan create –node <<var_nodeA>> -vlan-name e0e-
<<var_nfs_vlan_id>>
network port vlan create –node <<var_nodeA>> -vlan-name e0f-
<<var_nfs_vlan_id>>
network port vlan create –node <<var_nodeB>> -vlan-name e0e-
<<var_nfs_vlan_id>>
network port vlan create –node <<var_nodeB>> -vlan-name e0f-
<<var_nfs_vlan_id>>
broadcast-domain add-ports -broadcast-domain Infra_NFS -ports
<<var_nodeA>>: e0e- <<var_nfs_vlan_id>>, <<var_nodeB>>: e0e-
<<var_nfs_vlan_id>> , <<var_nodeA>>:e0f- <<var_nfs_vlan_id>>,
<<var_nodeB>>:e0f-<<var_nfs_vlan_id>>
```

2. iSCSI VLAN 포트를 생성하여 데이터 브로드캐스트 도메인에 추가합니다.

```
network port vlan create –node <<var_nodeA>> -vlan-name e0e-
<<var_iscsi_vlan_A_id>>
network port vlan create –node <<var_nodeA>> -vlan-name e0f-
<<var_iscsi_vlan_B_id>>
network port vlan create –node <<var_nodeB>> -vlan-name e0e-
<<var_iscsi_vlan_A_id>>
network port vlan create –node <<var_nodeB>> -vlan-name e0f-
<<var_iscsi_vlan_B_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-A -ports
<<var_nodeA>>: e0e- <<var_iscsi_vlan_A_id>>,<<var_nodeB>>: e0e-
<<var_iscsi_vlan_A_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-B -ports
<<var_nodeA>>: e0f- <<var_iscsi_vlan_B_id>>,<<var_nodeB>>: e0f-
<<var_iscsi_vlan_B_id>>
```

3. MGMT-VLAN 포트를 생성합니다.

```
network port vlan create –node <<var_nodeA>> -vlan-name e0m-
<<mgmt_vlan_id>>
network port vlan create –node <<var_nodeB>> -vlan-name e0m-
<<mgmt_vlan_id>>
```

ONTAP에서 애그리게이트를 생성합니다

ONTAP 설정 프로세스 중에 루트 볼륨이 포함된 애그리게이트가 생성됩니다. 추가 애그리게이트를 생성하려면 애그리게이트 이름, 애그리게이트를 생성할 노드, 애그리게이트에 포함된 디스크 수를 결정합니다.

Aggregate를 생성하려면 다음 명령을 실행합니다.

```
aggr create -aggregate aggr1_nodeA -node <<var_nodeA>> -diskcount
<<var_num_disks>>
aggr create -aggregate aggr1_nodeB -node <<var_nodeB>> -diskcount
<<var_num_disks>>
```

구성에 최소 하나의 디스크(가장 큰 디스크 선택)를 스페어로 보관합니다. 모범 사례는 각 디스크 유형 및 크기에 대해 하나 이상의 스페어를 두는 것입니다.

5개의 디스크로 시작합니다. 스토리지를 추가해야 할 때 디스크를 애그리게이트에 추가할 수 있습니다.

디스크 비우기가 완료될 때까지 애그리게이트를 생성할 수 없습니다. 집계 생성 상태를 표시하려면 'aggr show' 명령을 실행합니다. aggr1_NodeA가 온라인이 될 때까지 진행하지 마십시오.

ONTAP에서 시간대를 구성합니다

시간 동기화를 구성하고 클러스터에서 표준 시간대를 설정하려면 다음 명령을 실행합니다.

```
timezone <<var_timezone>>
```

예를 들어, 미국 동부의 시간대는 '아메리카/뉴욕'입니다. 표준 시간대 이름을 입력하기 시작하면 Tab 키를 눌러 사용 가능한 옵션을 확인합니다.

ONTAP에서 SNMP를 구성합니다

SNMP를 구성하려면 다음 단계를 수행하십시오.

1. 위치 및 연락처와 같은 SNMP 기본 정보를 구성합니다. 이 정보는 SNMP에서 'SysLocation', 'SysContact' 변수로 표시됩니다.

```
snmp contact <<var_snmp_contact>>
snmp location "<<var_snmp_location>>"
snmp init 1
options snmp.enable on
```

2. 원격 호스트에 보낼 SNMP 트랩을 구성합니다.

```
snmp traphost add <<var_snmp_server_fqdn>>
```

ONTAP에서 SNMPv1을 구성합니다

SNMPv1을 구성하려면 커뮤니티라는 공유 암호 일반 텍스트 암호를 설정합니다.

```
snmp community add ro <<var_snmp_community>>
```

NMP community delete all 명령을 주의하여 사용한다. 다른 모니터링 제품에 커뮤니티 문자열을 사용하는 경우 이 명령은 해당 문자열을 제거합니다.

ONTAP에서 SNMPv3을 구성합니다

SNMPv3을 사용하려면 인증을 위해 사용자를 정의하고 구성해야 합니다. SNMPv3을 구성하려면 다음 단계를 수행하십시오.

1. Security snmpusers 명령을 실행하여 엔진 ID를 조회한다.
2. 'snmpv3user'라는 사용자를 생성합니다.

```
security login create -username snmpv3user -authmethod usm -application
snmp
```

3. 신뢰할 수 있는 엔터티의 엔진 ID를 입력하고 인증 프로토콜로 md5 를 선택한다.
4. 메시지가 나타나면 인증 프로토콜에 사용할 최소 길이 8자로 된 암호를 입력합니다.
5. 개인 정보 보호 프로토콜로 'des'를 선택합니다.
6. 메시지가 나타나면 개인 정보 보호 프로토콜에 사용할 최소 길이 8자로 된 암호를 입력합니다.

ONTAP에서 **AutoSupport HTTPS**를 구성합니다

NetApp AutoSupport 툴은 HTTPS를 통해 지원 요약 정보를 NetApp에 보냅니다. AutoSupport를 구성하려면 다음 명령을 실행합니다.

```
system node autosupport modify -node * -state enable –mail-hosts
<<var_mailhost>> -transport https -support enable -noteto
<<var_storage_admin_email>>
```

스토리지 가상 머신을 생성합니다

인프라 스토리지 가상 시스템(SVM)을 생성하려면 다음 단계를 완료하십시오.

1. 'vserver create' 명령을 실행합니다.

```
vserver create –vserver Infra-SVM –rootvolume rootvol –aggregate
aggr1_nodeA –rootvolume- security-style unix
```

2. NetApp VSC를 위한 인프라-SVM 애그리게이트 목록에 데이터 애그리게이트를 추가합니다.

```
vserver modify -vserver Infra-SVM -aggr-list aggr1_nodeA,aggr1_nodeB
```

3. NFS와 iSCSI를 남겨두고 SVM에서 사용하지 않는 스토리지 프로토콜을 제거합니다.

```
vserver remove-protocols –vserver Infra-SVM -protocols cifs,ndmp,fcp
```

4. 인프라 SVM에서 NFS 프로토콜을 사용하고 실행합니다.

```
nfs create -vserver Infra-SVM -udp disabled
```

5. NetApp NFS VAAI 플러그인에 대한 'VM vStorage' 매개 변수를 설정합니다. 그런 다음 NFS가 구성되었는지 확인합니다.

```
vserver nfs modify -vserver Infra-SVM -vstorage enabled
vserver nfs show
```

SVM은 이전에 서버라고 불렸던 것이기 때문에 명령행에서 'vserver'가 명령을 앞에 표시합니다

ONTAP에서 **NFSv3**을 구성합니다

아래 표에는 이 구성을 완료하는 데 필요한 정보가 나와 있습니다.

세부 정보	상세 값
ESXi 호스트 NFS IP 주소입니다	<<var_esxi_hostA_nfs_ip>> 를 참조하십시오
ESXi 호스트 B NFS IP 주소입니다	<<var_esxi_hostB_nfs_ip>> 를 참조하십시오

SVM에서 NFS를 구성하려면 다음 명령을 실행합니다.

1. 기본 엑스포트 정책에서 각 ESXi 호스트에 대한 규칙을 생성합니다.
2. 생성 중인 각 ESXi 호스트에 대해 규칙을 할당합니다. 각 호스트에는 고유한 규칙 인덱스가 있습니다. 첫 번째 ESXi 호스트에는 규칙 인덱스 1이 있고 두 번째 ESXi 호스트에는 규칙 인덱스 2가 있습니다.

```
vserver export-policy rule create –vserver Infra-SVM -policyname default
–ruleindex 1 –protocol nfs -clientmatch <<var_esxi_hostA_nfs_ip>>
-rorule sys –rwrule sys -superuser sys –allow-suid falsevserver export-
policy rule create –vserver Infra-SVM -policyname default –ruleindex 2
-protocol nfs -clientmatch <<var_esxi_hostB_nfs_ip>> -rorule sys –rwrule
sys -superuser sys –allow-suid false
vserver export-policy rule show
```

3. 인프라 SVM 루트 볼륨에 엑스포트 정책을 할당합니다.

```
volume modify –vserver Infra-SVM –volume rootvol –policy default
```

vSphere를 설정한 후 NetApp VSC는 엑스포트 정책을 자동으로 처리합니다. 설치하지 않은 경우 Cisco UCS B-Series 서버를 추가할 때 엑스포트 정책 규칙을 생성해야 합니다.

ONTAP에서 **iSCSI** 서비스를 생성합니다

iSCSI 서비스를 생성하려면 다음 단계를 완료하십시오.

1. SVM에서 iSCSI 서비스를 생성합니다. 또한 이 명령은 iSCSI 서비스를 시작하고 SVM에 대한 IQN(iSCSI Qualified Name)을 설정합니다. iSCSI가 구성되었는지 확인합니다.

```
iscsi create -vserver Infra-SVM
iscsi show
```

ONTAP에서 SVM 루트 볼륨의 로드 공유 미러를 생성합니다

ONTAP에서 SVM 루트 볼륨의 로드 공유 미러를 생성하려면 다음 단계를 수행하십시오.

1. 각 노드에서 인프라 SVM 루트 볼륨의 로드 공유 미러가 될 볼륨을 생성합니다.

```
volume create –vserver Infra_Vserver –volume rootvol_m01 –aggregate
aggr1_nodeA –size 1GB –type DPvolume create –vserver Infra_Vserver
–volume rootvol_m02 –aggregate aggr1_nodeB –size 1GB –type DP
```

2. 15분마다 루트 볼륨 미러 관계를 업데이트하는 작업 스케줄을 생성합니다.

```
job schedule interval create -name 15min -minutes 15
```

3. 미러링 관계를 생성합니다.

```
snapmirror create -source-path Infra-SVM:rootvol -destination-path
Infra-SVM:rootvol_m01 -type LS -schedule 15min
snapmirror create -source-path Infra-SVM:rootvol -destination-path
Infra-SVM:rootvol_m02 -type LS -schedule 15min
```

4. 미러링 관계를 초기화하고 미러링 관계가 만들어졌는지 확인합니다.

```
snapmirror initialize-ls-set -source-path Infra-SVM:rootvol snapmirror
show
```

ONTAP에서 HTTPS 액세스를 구성합니다

스토리지 컨트롤러에 대한 보안 액세스를 구성하려면 다음 단계를 수행하십시오.

1. 인증서 명령에 액세스할 수 있도록 권한 수준을 높입니다.

```
set -privilege diag
Do you want to continue? {y|n}: y
```

2. 일반적으로 자체 서명된 인증서가 이미 있습니다. 다음 명령을 실행하여 인증서를 확인합니다.

```
security certificate show
```

3. 표시된 각 SVM에서 인증서 공통 이름은 SVM의 DNS FQDN(정규화된 도메인 이름)과 일치해야 합니다. 네 개의 기본 인증서를 삭제하고 자체 서명된 인증서 또는 인증 기관의 인증서로 대체해야 합니다.

   인증서를 만들기 전에 만료된 인증서를 삭제하는 것이 좋습니다. 만료된 인증서를 삭제하려면 보안 인증서 삭제 명령을 실행합니다. 다음 명령에서 Tab completion을 사용하여 각 기본 인증서를 선택하고 삭제합니다.

```
security certificate delete [TAB] ...
Example: security certificate delete -vserver Infra-SVM -common-name
Infra-SVM -ca Infra-SVM - type server -serial 552429A6
```

4. 자체 서명된 인증서를 생성하고 설치하려면 다음 명령을 일회성 명령으로 실행합니다. 인프라 SVM 및 클러스터 SVM에 대한 서버 인증서를 생성합니다. 다시 한 번 탭 완료 기능을 사용하면 이러한 명령을 쉽게 완료할 수 있습니다.

```
security certificate create [TAB] ...
Example: security certificate create -common-name infra-svm.netapp.com
-type server -size 2048 - country US -state "North Carolina" -locality
"RTP" -organization "NetApp" -unit "FlexPod" -email- addr
"abc@netapp.com" -expire-days 365 -protocol SSL -hash-function SHA256
-vserver Infra-SVM
```

5. 다음 단계에서 필요한 매개 변수 값을 얻으려면 'security certificate show' 명령을 실행합니다.
6. '–server-enabled true' 및 '–client-enabled false' 매개 변수를 사용하여 방금 만든 각 인증서를 활성화합니다. 다시 탭 완료를 사용합니다.

```
security ssl modify [TAB] ...
Example: security ssl modify -vserver Infra-SVM -server-enabled true
-client-enabled false -ca infra-svm.netapp.com -serial 55243646 -common
-name infra-svm.netapp.com
```

7. SSL 및 HTTPS 액세스를 구성 및 활성화하고 HTTP 액세스를 비활성화합니다.

```
system services web modify -external true -sslv3-enabled true
Warning: Modifying the cluster configuration will cause pending web
service requests to be interrupted as the web servers are restarted.
Do you want to continue {y|n}: y
System services firewall policy delete -policy mgmt -service http
-vserver <<var_clustername>>
```

명령 실행 중 일부에서 항목이 존재하지 않는다는 오류 메시지가 반환되는 것은 정상입니다.

8. 관리 권한 수준으로 되돌아가며 SVM을 웹에서 사용할 수 있도록 설정을 생성합니다.

```
set -privilege admin
vserver services web modify -name spi|ontapi|compat -vserver * -enabled
true
```

ONTAP에서 **NetApp FlexVol** 볼륨을 생성합니다

NetApp FlexVol ® 볼륨을 생성하려면 볼륨 이름, 크기 및 해당 볼륨을 입력합니다. 2개의 VMware 데이터 저장소 볼륨과 서버 부팅 볼륨을 생성합니다.

```
volume create -vserver Infra-SVM -volume infra_datastore_1 -aggregate
aggr1_nodeA -size 500GB - state online -policy default -junction-path
/infra_datastore_1 -space-guarantee none -percent- snapshot-space 0
volume create -vserver Infra-SVM -volume infra_datastore_2 -aggregate
aggr1_nodeB -size 500GB - state online -policy default -junction-path
/infra_datastore_2 -space-guarantee none -percent- snapshot-space 0
```

```
volume create -vserver Infra-SVM -volume infra_swap -aggregate aggr1_nodeA
-size 100GB -state online -policy default -juntion-path /infra_swap -space
-guarantee none -percent-snapshot-space 0 -snapshot-policy none
volume create -vserver Infra-SVM -volume esxi_boot -aggregate aggr1_nodeA
-size 100GB -state online -policy default -space-guarantee none -percent
-snapshot-space 0
```

ONTAP에서 중복 제거를 설정합니다

하루에 한 번 적절한 볼륨에서 중복 제거를 설정하려면 다음 명령을 실행합니다.

```
volume efficiency modify -vserver Infra-SVM -volume esxi_boot -schedule
sun-sat@0
volume efficiency modify -vserver Infra-SVM -volume infra_datastore_1
-schedule sun-sat@0
volume efficiency modify -vserver Infra-SVM -volume infra_datastore_2
-schedule sun-sat@0
```

ONTAP에서 **LUN**을 생성합니다

두 개의 부팅 논리 유닛 번호(LUN)를 생성하려면 다음 명령을 실행합니다.

```
lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-A -size
15GB -ostype vmware - space-reserve disabled
lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-B -size
15GB -ostype vmware - space-reserve disabled
```

Cisco UCS C-Series 서버를 더 추가할 때는 부팅 LUN을 더 생성해야 합니다.

ONTAP에서 **iSCSI LIF**를 생성합니다

아래 표에는 이 구성을 완료하는 데 필요한 정보가 나와 있습니다.

세부 정보	상세 값
스토리지 노드 A iSCSI LIF01A	<<var_NodeA_iscsi_lif01a_ip>> 를 참조하십시오
스토리지 노드 A iSCSI LIF01A 네트워크 마스크입니다	<<var_NodeA_iscsi_lif01a_mask>>
스토리지 노드 A iSCSI LIF01B	<<var_NodeA_iscsi_liff 01b_ip>> 를 참조하십시오
스토리지 노드 A iSCSI LIF01B 네트워크 마스크입니다	<<var_NodeA_iscsi_liff 01b_mask>>
스토리지 노드 B iSCSI LIF01A	<<var_NodeB_iscsi_liff 01a_ip>>
스토리지 노드 B iSCSI LIF01A 네트워크 마스크입니다	<<var_NodeB_iscsi_liff 01a_mask>>
스토리지 노드 B iSCSI LIF01B	<<var_NodeB_iscsi_liff 01b_ip>>
스토리지 노드 B iSCSI LIF01B 네트워크 마스크입니다	<<var_NodeB_iscsi_liff 01b_mask>>

1. 각 노드에 2개의 iSCSI LIF를 4개 생성합니다.

```
network interface create -vserver Infra-SVM -lif iscsi_lif01a -role data
-data-protocol iscsi - home-node <<var_nodeA>> -home-port e0e-
<<var_iscsi_vlan_A_id>> -address <<var_nodeA_iscsi_lif01a_ip>> -netmask
<<var_nodeA_iscsi_lif01a_mask>> –status-admin up – failover-policy
disabled –firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif01b -role data
-data-protocol iscsi - home-node <<var_nodeA>> -home-port e0f-
<<var_iscsi_vlan_B_id>> -address <<var_nodeA_iscsi_lif01b_ip>> -netmask
<<var_nodeA_iscsi_lif01b_mask>> –status-admin up – failover-policy
disabled –firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02a -role data
-data-protocol iscsi - home-node <<var_nodeB>> -home-port e0e-
<<var_iscsi_vlan_A_id>> -address <<var_nodeB_iscsi_lif01a_ip>> -netmask
<<var_nodeB_iscsi_lif01a_mask>> –status-admin up – failover-policy
disabled –firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02b -role data
-data-protocol iscsi - home-node <<var_nodeB>> -home-port e0f-
<<var_iscsi_vlan_B_id>> -address <<var_nodeB_iscsi_lif01b_ip>> -netmask
<<var_nodeB_iscsi_lif01b_mask>> –status-admin up – failover-policy
disabled –firewall-policy data –auto-revert false
network interface show
```

ONTAP에서 **NFS LIF**를 생성합니다

다음 표에는 이 구성을 완료하는 데 필요한 정보가 나와 있습니다.

세부 정보	상세 값
스토리지 노드 A NFS LIF 01 A IP	<<var_NodeA_nfs_lif_01_a_ip>>
스토리지 노드 A NFS LIF 01 네트워크 마스크입니다	<<var_NodeA_nfs_lif_01_a_mask>>
스토리지 노드 A NFS LIF 01 b IP입니다	<<var_NodeA_nfs_lif_01_b_ip>>
스토리지 노드 A NFS LIF 01 b 네트워크 마스크	<<var_NodeA_nfs_lif_01_b_mask>>
스토리지 노드 B NFS LIF 02 A IP	<<var_NodeB_nfs_lif_02_a_ip>>
스토리지 노드 B NFS LIF 02 A 네트워크 마스크	<<var_NodeB_nfs_lif_02_a_mask>>
스토리지 노드 B NFS LIF 02 b IP	<<var_NodeB_nfs_lif_02_b_ip>>
스토리지 노드 B NFS LIF 02 b 네트워크 마스크	<<var_NodeB_nfs_lif_02_b_mask>>

1. NFS LIF를 생성합니다.

```
network interface create -vserver Infra-SVM -lif nfs_lif01_a -role data
-data-protocol nfs -home- node <<var_nodeA>> -home-port e0e-
<<var_nfs_vlan_id>> -address <<var_nodeA_nfs_lif_01_a_ip>> - netmask <<
var_nodeA_nfs_lif_01_a_mask>> -status-admin up –failover-policy
broadcast-domain-wide – firewall-policy data –auto-revert true
network interface create -vserver Infra-SVM -lif nfs_lif01_b -role data
-data-protocol nfs -home- node <<var_nodeA>> -home-port e0f-
<<var_nfs_vlan_id>> -address <<var_nodeA_nfs_lif_01_b_ip>> - netmask <<
var_nodeA_nfs_lif_01_b_mask>> -status-admin up –failover-policy
broadcast-domain-wide – firewall-policy data –auto-revert true
network interface create -vserver Infra-SVM -lif nfs_lif02_a -role data
-data-protocol nfs -home- node <<var_nodeB>> -home-port e0e-
<<var_nfs_vlan_id>> -address <<var_nodeB_nfs_lif_02_a_ip>> - netmask <<
var_nodeB_nfs_lif_02_a_mask>> -status-admin up –failover-policy
broadcast-domain-wide – firewall-policy data –auto-revert true
network interface create -vserver Infra-SVM -lif nfs_lif02_b -role data
-data-protocol nfs -home- node <<var_nodeB>> -home-port e0f-
<<var_nfs_vlan_id>> -address <<var_nodeB_nfs_lif_02_b_ip>> - netmask <<
var_nodeB_nfs_lif_02_b_mask>> -status-admin up –failover-policy
broadcast-domain-wide – firewall-policy data –auto-revert true
network interface show
```

인프라 **SVM** 관리자를 추가합니다

다음 표에는 이 구성을 완료하는 데 필요한 정보가 나와 있습니다.

세부 정보	상세 값
Vsmgmt IP	<<var_svm_mgmt_ip>> 를 입력합니다
Vsmgmt 네트워크 마스크	<<var_svm_mgmt_mask>>
Vsmgmt 기본 게이트웨이	<<var_svm_mgmt_gateway>>

인프라 SVM 관리자 및 SVM 관리 LIF를 관리 네트워크에 추가하려면 다음 단계를 완료하십시오.

1. 다음 명령을 실행합니다.

```
network interface create –vserver Infra-SVM –lif vsmgmt –role data
–data-protocol none –home-node <<var_nodeB>> -home-port e0M –address
<<var_svm_mgmt_ip>> -netmask <<var_svm_mgmt_mask>> - status-admin up
–failover-policy broadcast-domain-wide –firewall-policy mgmt –auto-
revert true
```

ⓘ 여기서 SVM 관리 IP는 스토리지 클러스터 관리 IP와 동일한 서브넷에 있어야 합니다.

2. 기본 경로를 생성하여 SVM 관리 인터페이스가 외부 환경에 도달할 수 있도록 합니다.

```
network route create –vserver Infra-SVM -destination 0.0.0.0/0 –gateway
<<var_svm_mgmt_gateway>> network route show
```

3. SVM 'vsadmin' 사용자의 비밀번호를 설정하고 사용자 잠금을 해제합니다.

```
security login password –username vsadmin –vserver Infra-SVM
Enter a new password: <<var_password>>
Enter it again: <<var_password>>
security login unlock –username vsadmin –vserver
```

Cisco UCS 서버 구성

FlexPod Cisco UCS 기반

FlexPod 환경을 위한 Cisco UCS 6324 패브릭 인터커넥트를 초기 설정합니다.

이 섹션에서는 Cisco UCS Manger를 사용하여 FlexPod ROBO 환경에서 Cisco UCS를 사용하도록 구성하는 절차를 자세히 설명합니다.

Cisco UCS 패브릭 인터커넥트 6324 A

Cisco UCS는 액세스 계층 네트워킹 및 서버를 사용합니다. 이 고성능 차세대 서버 시스템은 데이터 센터에 높은 수준의 워크로드 민첩성 및 확장성을 제공합니다.

Cisco UCS Manager 4.0(1b)은 패브릭 인터커넥트를 Cisco UCS 섀시에 통합하고 더 작은 구축 환경을 위한 통합 솔루션을 제공하는 6324 패브릭 인터커넥트를 지원합니다. Cisco UCS Mini는 시스템 관리를 단순화하고 저렴한 배포 비용을 절감해 줍니다.

하드웨어 및 소프트웨어 구성 요소는 단일 통합 네트워크 어댑터를 통해 여러 유형의 데이터 센터 트래픽을 실행하는 Cisco의 통합 패브릭을 지원합니다.

초기 시스템 설치

Cisco UCS 도메인에서 패브릭 인터커넥트에 처음 액세스할 때 설정 마법사가 시스템을 구성하는 데 필요한 다음 정보를 묻습니다.

- 설치 방법(GUI 또는 CLI)
- 설정 모드(전체 시스템 백업 또는 초기 설정에서 복원)
- 시스템 구성 유형(독립 실행형 또는 클러스터 구성)
- 시스템 이름입니다
- 관리자 암호입니다
- 관리 포트 IPv4 주소 및 서브넷 마스크, 또는 IPv6 주소 및 접두어
- 기본 게이트웨이 IPv4 또는 IPv6 주소입니다

- DNS 서버 IPv4 또는 IPv6 주소입니다
- 기본 도메인 이름입니다

다음 표에는 Fabric Interconnect A에서 Cisco UCS 초기 구성을 완료하는 데 필요한 정보가 나와 있습니다

세부 정보	상세/값
시스템 이름	<<var_UCS_clustername>>
관리자 암호	<<var_password>> 를 참조하십시오
관리 IP 주소: 패브릭 인터커넥트 A	<<var_ucsa_mgmt_ip>> 를 입력합니다
관리 넷마스크: Fabric Interconnect A	<<var_ucsa_mgmt_mask>>
기본 게이트웨이: Fabric Interconnect A	<<var_ucsa_mgmt_gateway>>
클러스터 IP 주소입니다	<<var_UCS_cluster_ip>> 를 참조하십시오
DNS 서버 IP 주소입니다	<<var_nameserver_ip>> 를 참조하십시오
도메인 이름	<<var_domain_name>>

FlexPod 환경에서 사용할 Cisco UCS를 구성하려면 다음 단계를 완료하십시오.

1. 첫 번째 Cisco UCS 6324 Fabric Interconnect A의 콘솔 포트에 연결합니다

```
Enter the configuration method. (console/gui) ? console

  Enter the setup mode; setup newly or restore from backup.
(setup/restore) ? setup

  You have chosen to setup a new Fabric interconnect. Continue? (y/n): y

  Enforce strong password? (y/n) [y]: Enter

  Enter the password for "admin":<<var_password>>
  Confirm the password for "admin":<<var_password>>

  Is this Fabric interconnect part of a cluster(select 'no' for
standalone)? (yes/no) [n]: yes

  Enter the switch fabric (A/B) []: A

  Enter the system name: <<var_ucs_clustername>>

  Physical Switch Mgmt0 IP address : <<var_ucsa_mgmt_ip>>

  Physical Switch Mgmt0 IPv4 netmask : <<var_ucsa_mgmt_mask>>

  IPv4 address of the default gateway : <<var_ucsa_mgmt_gateway>>

  Cluster IPv4 address : <<var_ucs_cluster_ip>>

  Configure the DNS Server IP address? (yes/no) [n]: y

       DNS IP address : <<var_nameserver_ip>>

  Configure the default domain name? (yes/no) [n]: y
Default domain name: <<var_domain_name>>

  Join centralized management environment (UCS Central)? (yes/no) [n]:
no

 NOTE: Cluster IP will be configured only after both Fabric
Interconnects are initialized. UCSM will be functional only after peer
FI is configured in clustering mode.

  Apply and save the configuration (select 'no' if you want to re-
enter)? (yes/no): yes
  Applying configuration. Please wait.

  Configuration file - Ok
```

2. 콘솔에 표시된 설정을 검토합니다. 맞으면 yes로 답하여 설정을 적용하고 저장합니다.
3. 로그인 프롬프트가 구성을 저장했는지 확인할 때까지 기다립니다.

다음 표에는 Fabric Interconnect B에서 Cisco UCS 초기 구성을 완료하는 데 필요한 정보가 나와 있습니다

세부 정보	상세/값
시스템 이름	<<var_UCS_clustername>>
관리자 암호	<<var_password>> 를 참조하십시오
관리 IP 주소 - FI B	<<var_ucsb_mgmt_ip>> 를 입력합니다
관리 넷마스크 - FI B	<<var_ucsb_mgmt_mask>>
기본 게이트웨이 - FI B	<<var_ucsb_mgmt_gateway>>
클러스터 IP 주소입니다	<<var_UCS_cluster_ip>> 를 참조하십시오
DNS 서버 IP 주소입니다	<<var_nameserver_ip>> 를 참조하십시오
도메인 이름	<<var_domain_name>>

1. 두 번째 Cisco UCS 6324 Fabric Interconnect B의 콘솔 포트에 연결합니다

```
 Enter the configuration method. (console/gui) ? console

  Installer has detected the presence of a peer Fabric interconnect.
This Fabric interconnect will be added to the cluster. Continue (y/n) ?
y

  Enter the admin password of the peer Fabric
interconnect:<<var_password>>
    Connecting to peer Fabric interconnect... done
    Retrieving config from peer Fabric interconnect... done
    Peer Fabric interconnect Mgmt0 IPv4 Address: <<var_ucsb_mgmt_ip>>
    Peer Fabric interconnect Mgmt0 IPv4 Netmask: <<var_ucsb_mgmt_mask>>
    Cluster IPv4 address: <<var_ucs_cluster_address>>

    Peer FI is IPv4 Cluster enabled. Please Provide Local Fabric
Interconnect Mgmt0 IPv4 Address

  Physical Switch Mgmt0 IP address : <<var_ucsb_mgmt_ip>>


  Apply and save the configuration (select 'no' if you want to re-
enter)? (yes/no): yes
  Applying configuration. Please wait.

  Configuration file - Ok
```

2. 로그인 프롬프트가 구성을 저장했는지 확인할 때까지 기다립니다.

Cisco UCS Manager에 로그인합니다

Cisco UCS(Unified Computing System) 환경에 로그인하려면 다음 단계를 수행하십시오.

1. 웹 브라우저를 열고 Cisco UCS Fabric Interconnect 클러스터 주소로 이동합니다.

   Cisco UCS Manager가 나타날 수 있도록 두 번째 패브릭 인터커넥트를 구성한 후 5분 이상 기다려야 할 수 있습니다.

2. Cisco UCS Manager 실행 링크를 클릭하여 Cisco UCS Manager를 시작합니다.
3. 필요한 보안 인증서를 수락합니다.
4. 메시지가 표시되면 사용자 이름으로 admin 을 입력하고 관리자 암호를 입력합니다.
5. Cisco UCS Manager에 로그인하려면 로그인을 클릭합니다.

Cisco UCS Manager 소프트웨어 버전 **4.0(1b)**

이 문서에서는 Cisco UCS Manager 소프트웨어 버전 4.0(1b)을 사용한다고 가정합니다. Cisco UCS Manager 소프트웨어 및 Cisco UCS 6324 Fabric Interconnect 소프트웨어를 업그레이드하려면 을 참조하십시오 "Cisco UCS Manager 설치 및 업그레이드 가이드:"

Cisco UCS Call Home을 구성합니다

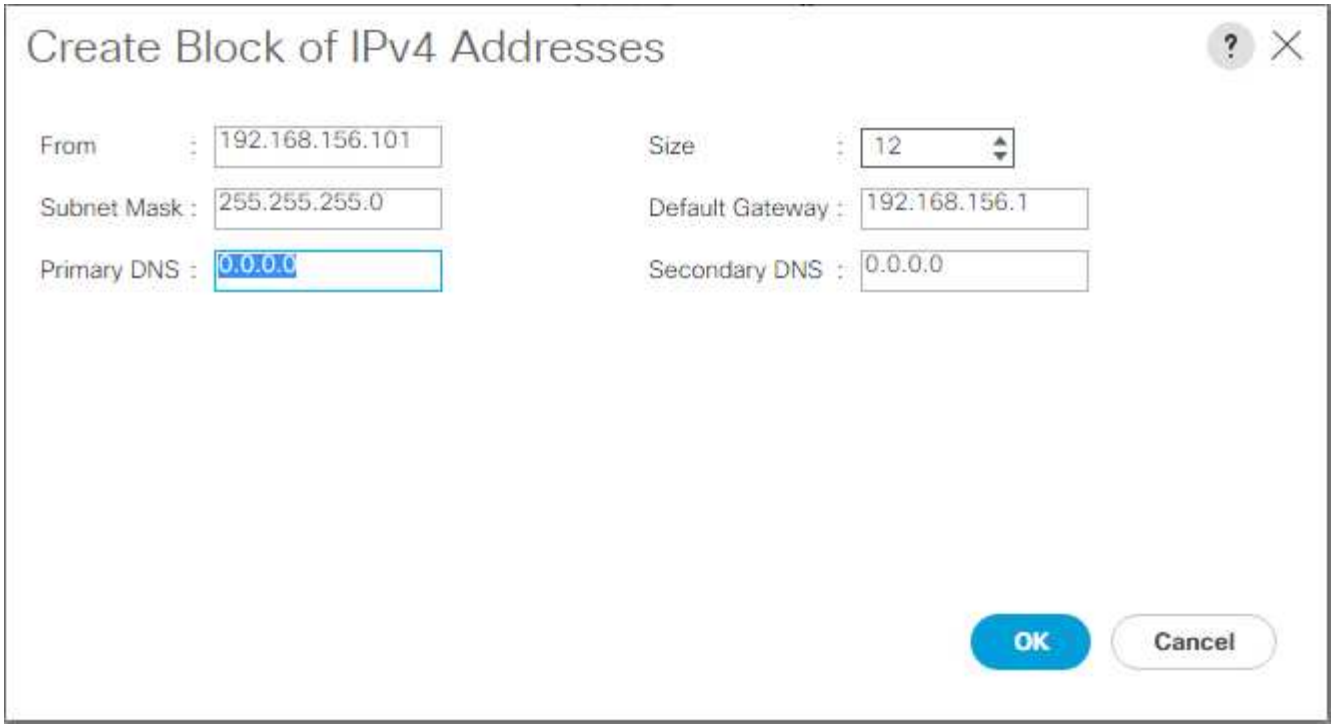
Cisco UCS Manager에서 Call Home을 구성하는 것이 좋습니다. Call Home을 구성하면 지원 케이스의 해결 속도가 빨라집니다. Call Home을 구성하려면 다음 단계를 수행하십시오.

1. Cisco UCS Manager의 경우 왼쪽에서 관리 를 클릭합니다.
2. 모두 > 통신 관리 > Call Home을 선택합니다.
3. 상태를 켜짐 으로 변경합니다.
4. Management(관리) 기본 설정에 따라 모든 필드를 입력하고 Save Changes(변경 사항 저장) 및 OK(확인) 를 클릭하여 Call Home 구성을 완료합니다.

키보드, 비디오, 마우스 액세스를 위한 **IP** 주소 블록을 추가합니다

Cisco UCS 환경에서 대역내 서버 키보드, 비디오, 마우스(KVM) 액세스를 위한 IP 주소 블록을 만들려면 다음 단계를 수행하십시오.

1. Cisco UCS Manager의 경우 왼쪽에 있는 LAN을 클릭합니다.
2. Pools > root > IP Pools 를 확장합니다.
3. IP Pool ext-mgmt 를 마우스 오른쪽 단추로 클릭하고 IPv4 주소 블록 만들기 를 선택합니다.
4. 블록의 시작 IP 주소, 필요한 IP 주소 수, 서브넷 마스크 및 게이트웨이 정보를 입력합니다.



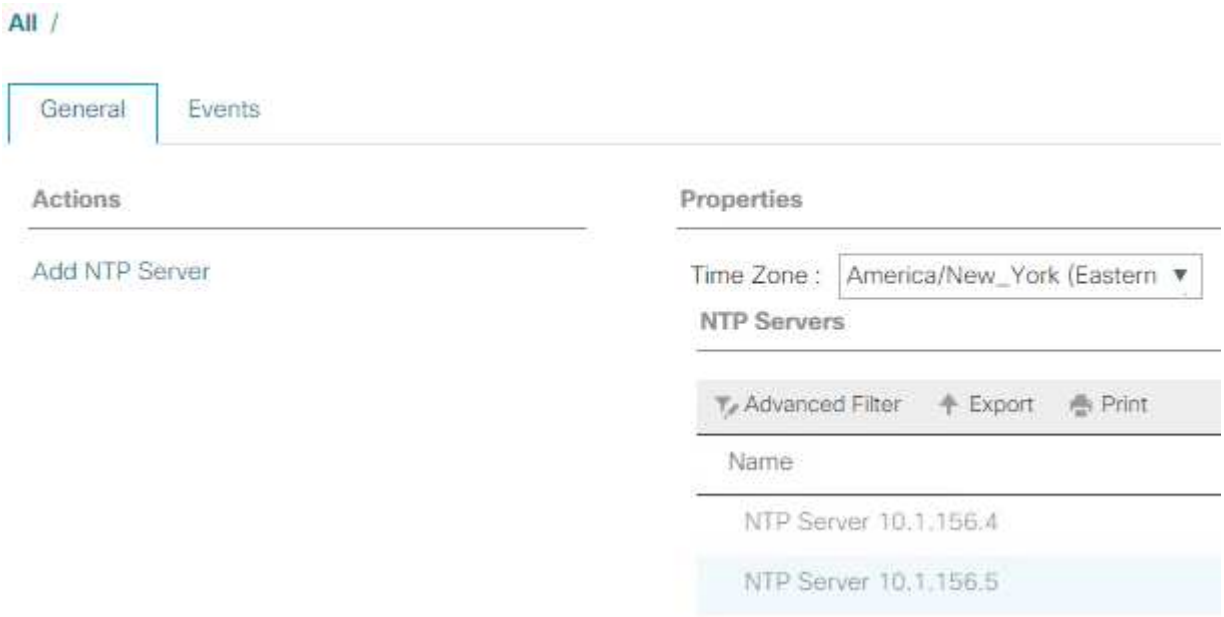
5. 확인 을 클릭하여 블럭을 작성합니다.
6. 확인 메시지에서 확인 을 클릭합니다.

Cisco UCS를 NTP에 동기화합니다

Cisco UCS 환경을 Nexus 스위치의 NTP 서버와 동기화하려면 다음 단계를 완료하십시오.

1. Cisco UCS Manager의 경우 왼쪽에서 관리 를 클릭합니다.
2. 모두 > 시간대 관리 를 확장합니다.
3. 시간대 를 선택합니다.
4. 속성 창의 표준 시간대 메뉴에서 적절한 시간대를 선택합니다.
5. 변경 내용 저장 을 클릭하고 확인 을 클릭합니다.
6. NTP 서버 추가를 클릭합니다.
7. '<switch-a-ntp-ip> 또는 <Nexus-a-mgmt-ip>'를 입력하고 확인을 클릭합니다. 확인 을 클릭합니다.

8. NTP 서버 추가를 클릭합니다.
9. '<switch-b-ntp-ip>' 또는 <Nexus-B-mgmt-ip>'를 입력하고 확인을 클릭합니다. 확인 창에서 확인 을 클릭합니다.



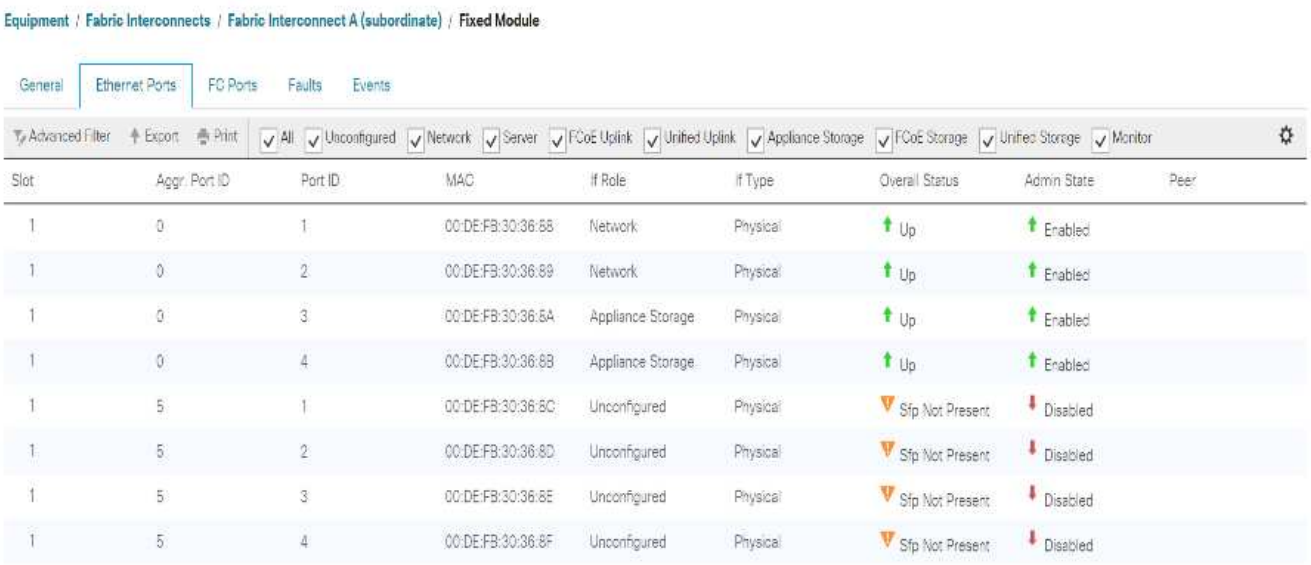
섀시 검색 정책을 편집합니다

검색 정책을 설정하면 Cisco UCS B-Series 섀시와 추가 패브릭 익스텐더를 간편하게 추가하여 Cisco UCS C-Series에 연결할 수 있습니다. 섀시 검색 정책을 수정하려면 다음 단계를 수행하십시오.

1. Cisco UCS Manager의 왼쪽에서 장비 를 클릭하고 두 번째 목록에서 장비 를 선택합니다.
2. 오른쪽 창에서 Policies 탭을 선택합니다.
3. 글로벌 정책에서 섀시/FEX 검색 정책을 섀시 또는 패브릭 익스텐더(FEX)와 패브릭 인터커넥트 간에 케이블로 연결된 최소 업링크 포트 수와 일치하도록 설정합니다.
4. 링크 그룹화 기본 설정을 포트 채널로 설정합니다. 설정 중인 환경에 많은 양의 멀티캐스트 트래픽이 포함된 경우 멀티캐스트 하드웨어 해시 설정을 사용으로 설정합니다.
5. 변경 내용 저장 을 클릭합니다.
6. 확인 을 클릭합니다.

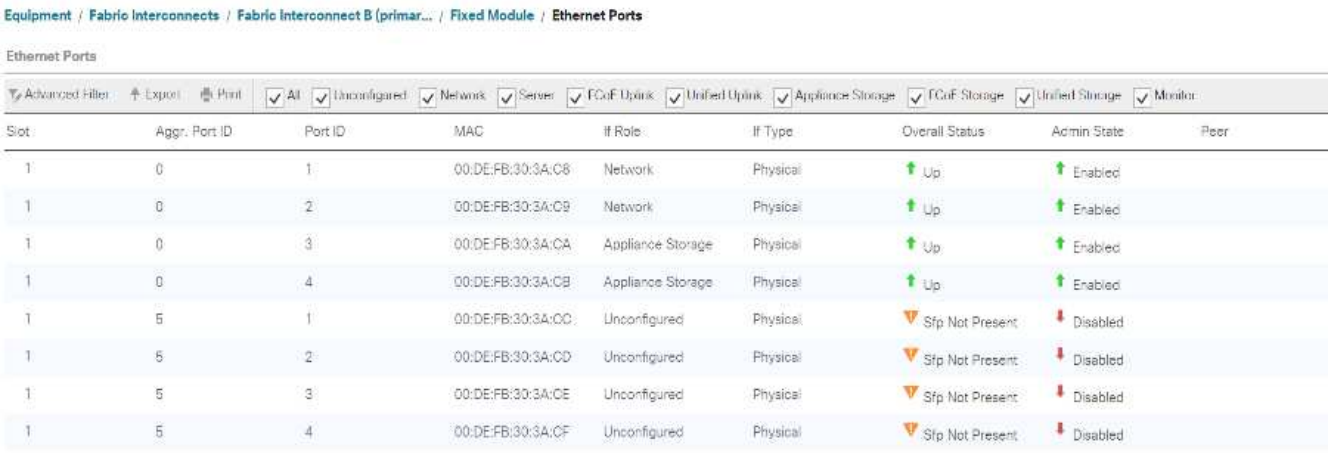
서버 및 업링크 포트를 활성화하려면 다음 단계를 수행하십시오.

1. Cisco UCS Manager의 탐색 창에서 장비 탭을 선택합니다.
2. 장비 > 패브릭 인터커넥트 > 패브릭 인터커넥트 A > 고정 모듈 을 확장합니다.
3. 이더넷 포트 를 확장합니다.
4. Cisco Nexus 31108 스위치에 연결된 포트 1과 2를 선택하고 마우스 오른쪽 단추를 클릭한 다음 업링크 포트로 구성 을 선택합니다.
5. 업링크 포트를 확인하려면 예를 클릭하고 확인을 클릭하십시오.
6. NetApp 스토리지 컨트롤러에 연결된 포트 3 및 4를 선택하고 마우스 오른쪽 버튼을 클릭한 다음 Configure as Appliance Port를 선택합니다.
7. 예 를 클릭하여 어플라이언스 포트를 확인합니다.
8. Configure as Appliance Port 창에서 OK를 클릭합니다.
9. 확인을 클릭하여 확인합니다.
10. 왼쪽 창에서 Fabric Interconnect A 아래에서 고정 모듈을 선택합니다
11. 이더넷 포트 탭의 IF 역할 열에서 포트가 올바르게 구성되었는지 확인합니다. 확장 포트에서 포트 C-Series 서버가 구성된 경우 해당 포트를 클릭하여 포트 연결을 확인합니다.



12. 장비 > 패브릭 인터커넥트 > 패브릭 인터커넥트 B > 고정 모듈 을 확장합니다.
13. 이더넷 포트 를 확장합니다.
14. Cisco Nexus 31108 스위치에 연결된 이더넷 포트 1과 2를 선택하고 마우스 오른쪽 버튼을 클릭한 다음 업링크 포트로 구성 을 선택합니다.
15. 업링크 포트를 확인하려면 예를 클릭하고 확인을 클릭하십시오.
16. NetApp 스토리지 컨트롤러에 연결된 포트 3 및 4를 선택하고 마우스 오른쪽 버튼을 클릭한 다음 Configure as Appliance Port를 선택합니다.
17. 예 를 클릭하여 어플라이언스 포트를 확인합니다.

18. Configure as Appliance Port 창에서 OK를 클릭합니다.
19. 확인을 클릭하여 확인합니다.
20. 왼쪽 창에서 Fabric Interconnect B 아래에서 고정 모듈을 선택합니다
21. 이더넷 포트 탭의 IF 역할 열에서 포트가 올바르게 구성되었는지 확인합니다. 확장 포트에서 포트 C-Series 서버가 구성된 경우 이를 클릭하여 포트 연결을 확인합니다.



Slot	Aggr. Port ID	Port ID	MAC	If Role	If Type	Overall Status	Admin State	Peer
1	0	1	00:DE:FB:30:3A:C8	Network	Physical	Up	Enabled	
1	0	2	00:DE:FB:30:3A:C9	Network	Physical	Up	Enabled	
1	0	3	00:DE:FB:30:3A:CA	Appliance Storage	Physical	Up	Enabled	
1	0	4	00:DE:FB:30:3A:CB	Appliance Storage	Physical	Up	Enabled	
1	5	1	00:DE:FB:30:3A:CC	Unconfigured	Physical	Sfp Not Present	Disabled	
1	5	2	00:DE:FB:30:3A:CD	Unconfigured	Physical	Sfp Not Present	Disabled	
1	5	3	00:DE:FB:30:3A:CE	Unconfigured	Physical	Sfp Not Present	Disabled	
1	5	4	00:DE:FB:30:3A:CF	Unconfigured	Physical	Sfp Not Present	Disabled	

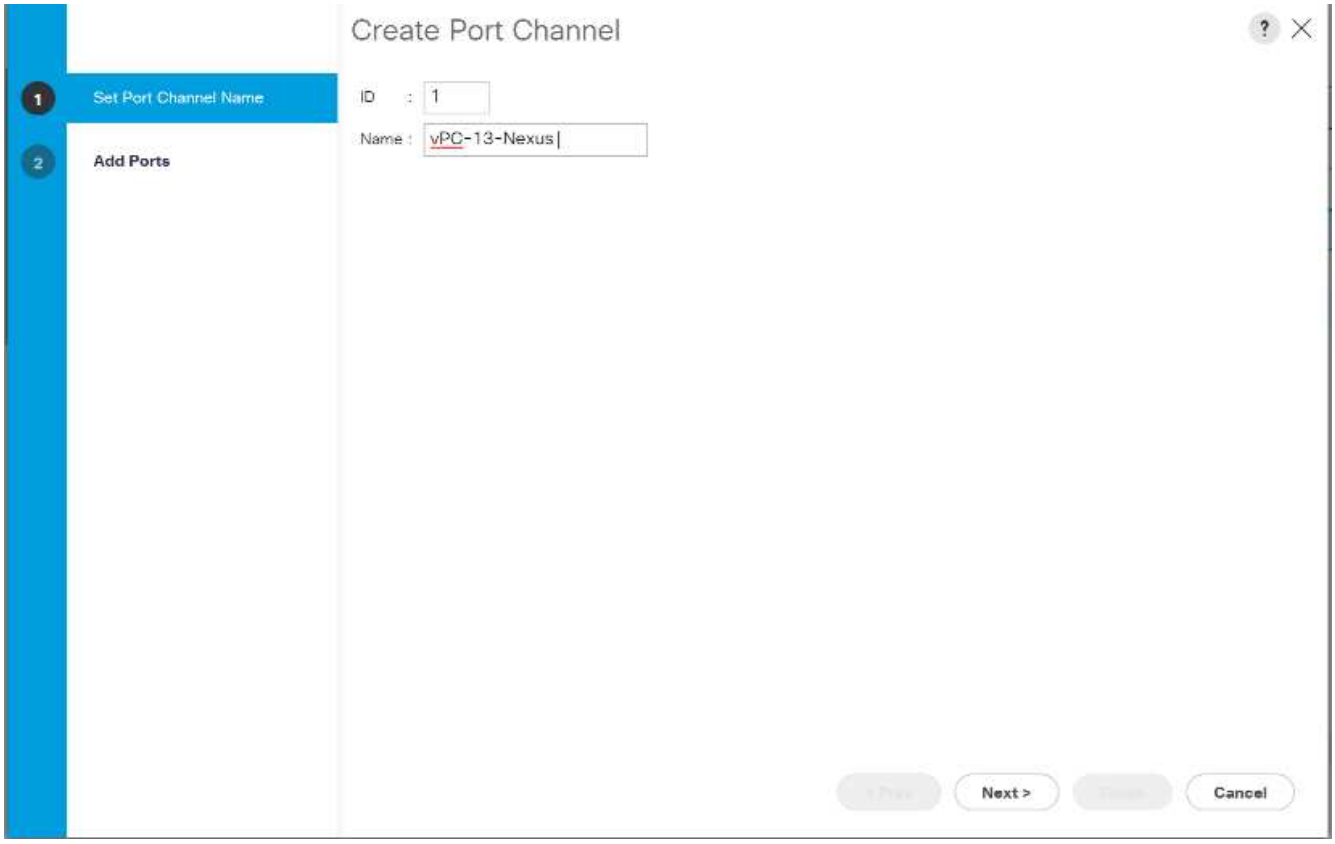
Cisco Nexus 31108 스위치에 업링크 포트 채널을 생성합니다

Cisco UCS 환경에서 필요한 포트 채널을 구성하려면 다음 단계를 수행하십시오.

1. Cisco UCS Manager의 탐색 창에서 LAN 탭을 선택합니다.

> 이 절차에서는 패브릭 A에서 Cisco Nexus 31108 스위치 두 개, 그리고 패브릭 B에서 Cisco Nexus 31108 스위치 두 개로 포트 채널 두 개가 생성됩니다. 표준 스위치를 사용하는 경우 이 절차를 적절히 수정합니다. 패브릭 인터커넥트에 1기가비트 이더넷(1GbE) 스위치 및 GLC-T SFP를 사용하는 경우 패브릭 상호 연결의 이더넷 포트 1/1 및 1/2의 인터페이스 속도를 1Gbps로 설정해야 합니다.

2. LAN > LAN 클라우드 에서 패브릭 A 트리를 확장합니다.
3. 포트 채널 을 마우스 오른쪽 단추로 클릭합니다.
4. 포트 채널 생성 을 선택합니다.
5. 포트 채널의 고유 ID로 13을 입력합니다.
6. 포트 채널 이름으로 vPC-13-Nexus를 입력합니다.
7. 다음 을 클릭합니다.



8. 포트 채널에 추가할 다음 포트를 선택합니다.
   a. 슬롯 ID 1 및 포트 1
   b. 슬롯 ID 1 및 포트 2
9. 포트 채널에 포트를 추가하려면 >> 를 클릭합니다.
10. 마침 을 클릭하여 포트 채널을 생성합니다. 확인 을 클릭합니다.
11. 포트 채널 에서 새로 생성된 포트 채널을 선택합니다.

    포트 채널은 전체 상태가 UP 이어야 합니다.

12. 탐색 창의 LAN > LAN Cloud 아래에서 패브릭 B 트리를 확장합니다.
13. 포트 채널 을 마우스 오른쪽 단추로 클릭합니다.
14. 포트 채널 생성 을 선택합니다.
15. 포트 채널의 고유 ID로 14를 입력합니다.
16. 포트 채널 이름으로 vPC-14-Nexus를 입력합니다. 다음 을 클릭합니다.
17. 포트 채널에 추가할 다음 포트를 선택합니다.
   a. 슬롯 ID 1 및 포트 1
   b. 슬롯 ID 1 및 포트 2
18. 포트 채널에 포트를 추가하려면 >> 를 클릭합니다.
19. 마침 을 클릭하여 포트 채널을 생성합니다. 확인 을 클릭합니다.
20. 포트 채널 에서 새로 생성된 포트 채널을 선택합니다.

21. 포트 채널은 전체 상태가 UP 이어야 합니다.

조직 만들기(선택 사항)

조직은 리소스를 구성하고 IT 조직 내의 다양한 그룹에 대한 액세스를 제한하여 컴퓨팅 리소스에 대한 멀티 테넌시를 활성화하는 데 사용됩니다.

> 이 문서에서는 조직의 사용을 전제로 하지 않지만 이 절차에서는 조직을 만드는 방법에 대한 지침을 제공합니다.

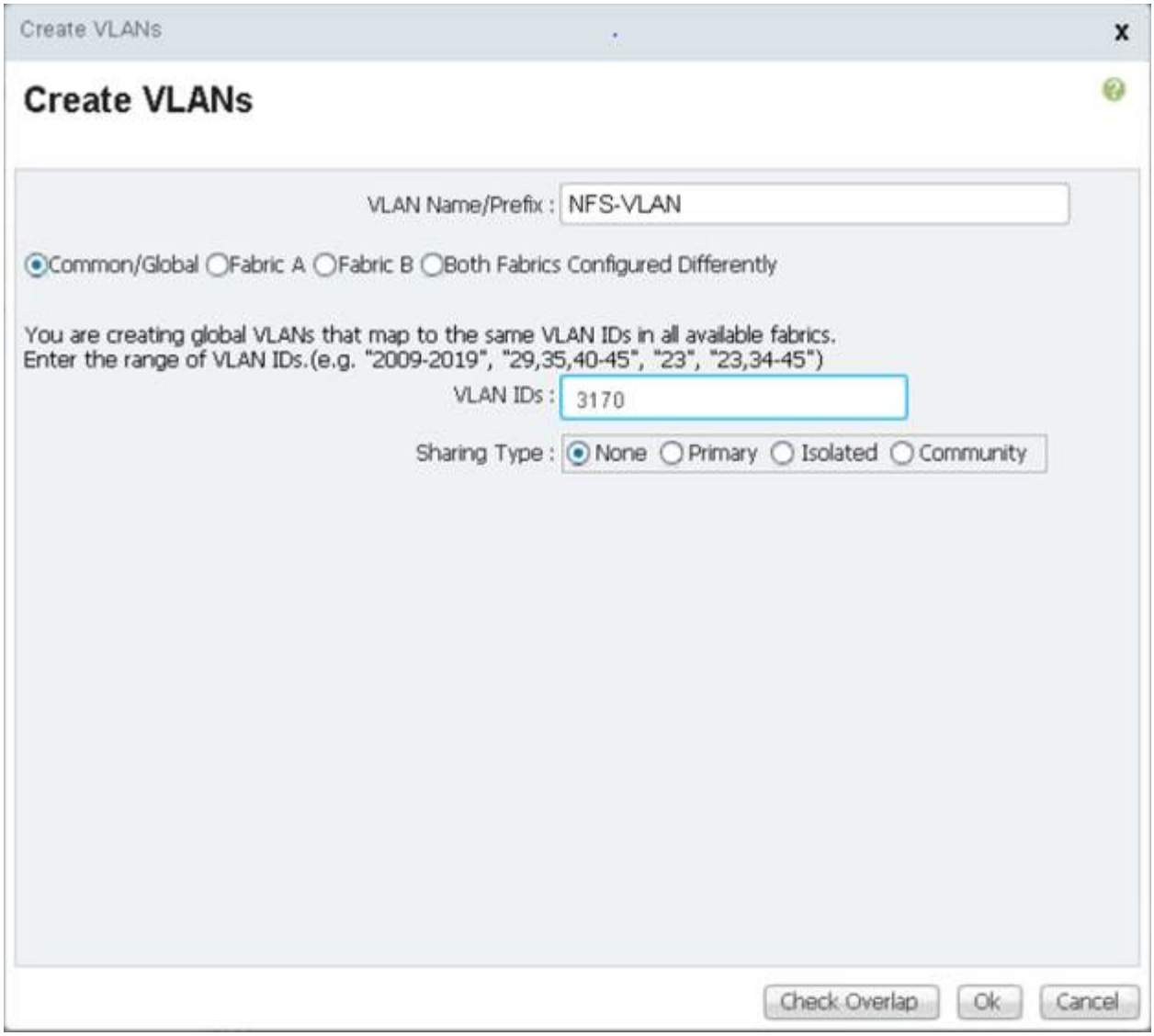
Cisco UCS 환경에서 조직을 구성하려면 다음 단계를 수행하십시오.

1. Cisco UCS Manager의 창 맨 위에 있는 도구 모음의 새로 만들기 메뉴에서 조직 만들기 를 선택합니다.
2. 조직의 이름을 입력합니다.
3. 선택 사항: 조직에 대한 설명을 입력합니다. 확인 을 클릭합니다.
4. 확인 메시지에서 확인 을 클릭합니다.

스토리지 어플라이언스 포트 및 스토리지 **VLAN**을 구성합니다

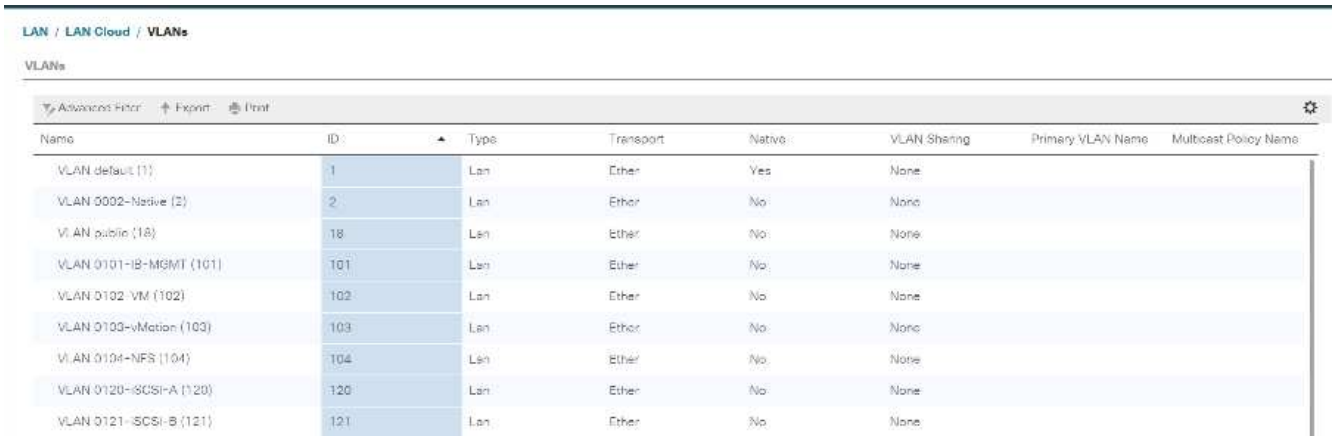
스토리지 어플라이언스 포트 및 스토리지 VLAN을 구성하려면 다음 단계를 수행하십시오.

1. Cisco UCS Manager에서 LAN 탭을 선택합니다.
2. 어플라이언스 클라우드 확장
3. Appliances Cloud 아래에서 VLAN을 마우스 오른쪽 버튼으로 클릭합니다.
4. VLAN 생성을 선택합니다.
5. 인프라스트럭처 NFS VLAN의 이름으로 NFS-VLAN을 입력합니다.
6. 공통/전체 를 선택한 상태로 둡니다.
7. VLAN ID에 '<<var_nfs_vlan_id>>'를 입력합니다.
8. 공유 유형을 없음으로 둡니다.

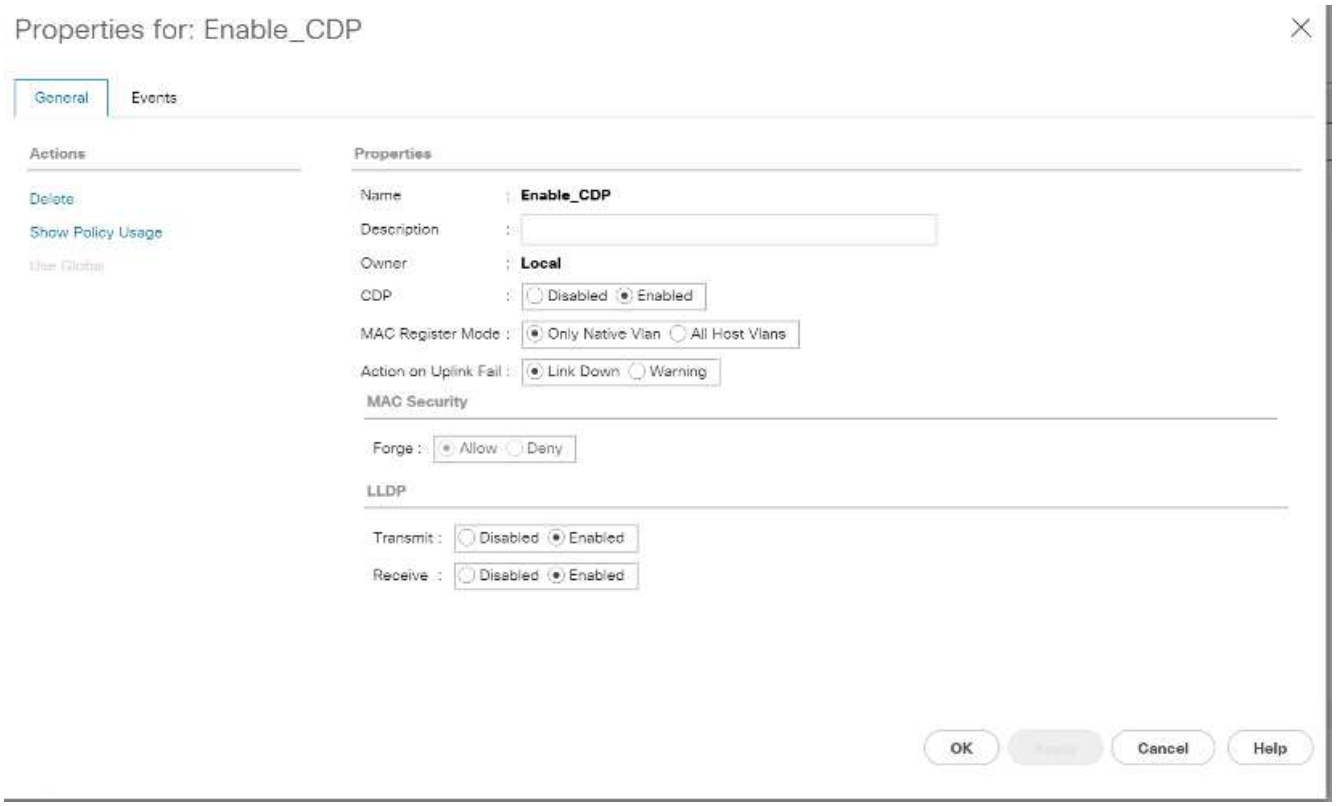


9. 확인을 클릭한 다음 확인을 다시 클릭하여 VLAN을 만듭니다.
10. Appliances Cloud 아래에서 VLAN을 마우스 오른쪽 버튼으로 클릭합니다.
11. VLAN 생성을 선택합니다.
12. 인프라 iSCSI 패브릭 A VLAN의 이름으로 iSCSI-A-VLAN을 입력합니다.
13. 공통/전체 를 선택한 상태로 둡니다.
14. VLAN ID에 '<<var_iscsi-a_vlan_id>>'를 입력합니다.
15. 확인을 클릭한 다음 확인을 다시 클릭하여 VLAN을 만듭니다.
16. Appliances Cloud 아래에서 VLAN을 마우스 오른쪽 버튼으로 클릭합니다.
17. VLAN 생성을 선택합니다.
18. 인프라 iSCSI 패브릭 B VLAN의 이름으로 iSCSI-B-VLAN을 입력합니다.
19. 공통/전체 를 선택한 상태로 둡니다.
20. VLAN ID에 '<<var_iscsi-b_vlan_id>>'를 입력합니다.
21. 확인을 클릭한 다음 확인을 다시 클릭하여 VLAN을 만듭니다.

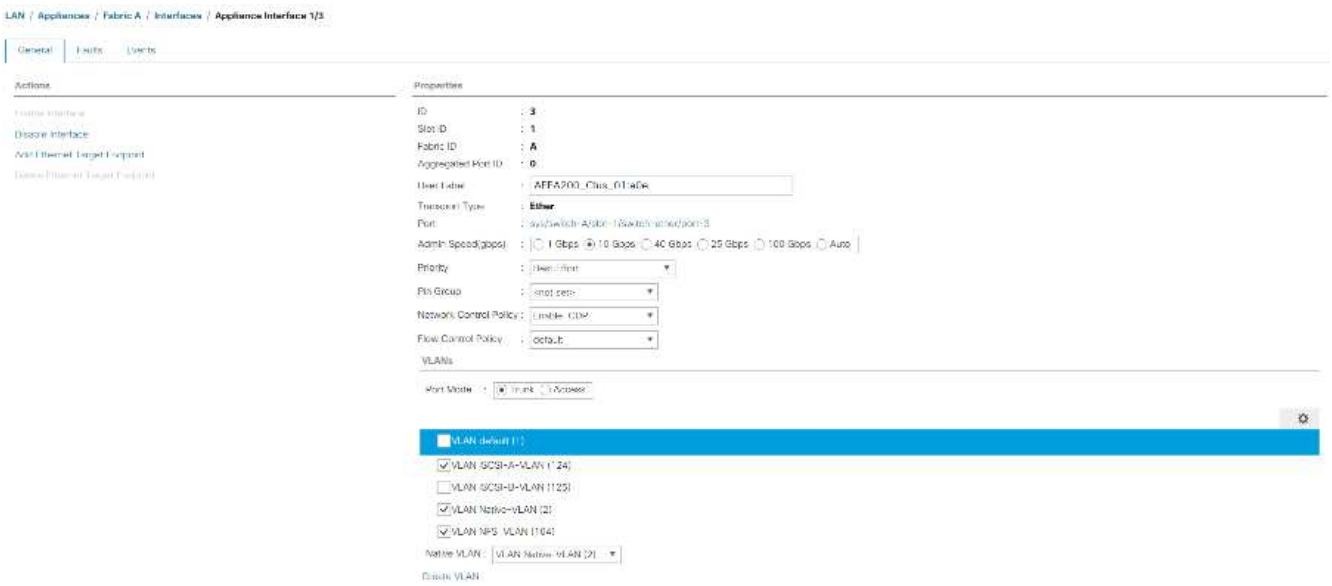
22. Appliances Cloud 아래에서 VLAN을 마우스 오른쪽 버튼으로 클릭합니다.
23. VLAN 생성을 선택합니다.
24. Native VLAN의 이름으로 Native-VLAN을 입력한다.
25. 공통/전체 를 선택한 상태로 둡니다.
26. VLAN ID에 '<<var_native_vlan_id>>'를 입력합니다.
27. 확인을 클릭한 다음 확인을 다시 클릭하여 VLAN을 만듭니다.



28. 탐색 창의 LAN > 정책 에서 어플라이언스 를 확장하고 네트워크 제어 정책 을 마우스 오른쪽 단추로 클릭합니다.
29. 네트워크 제어 정책 생성 을 선택합니다.
30. 정책 이름을 "Enable_CDP_LLPD"로 지정하고 CDP 옆에 있는 Enabled를 선택합니다.
31. LLDP의 전송 및 수신 기능을 활성화합니다.

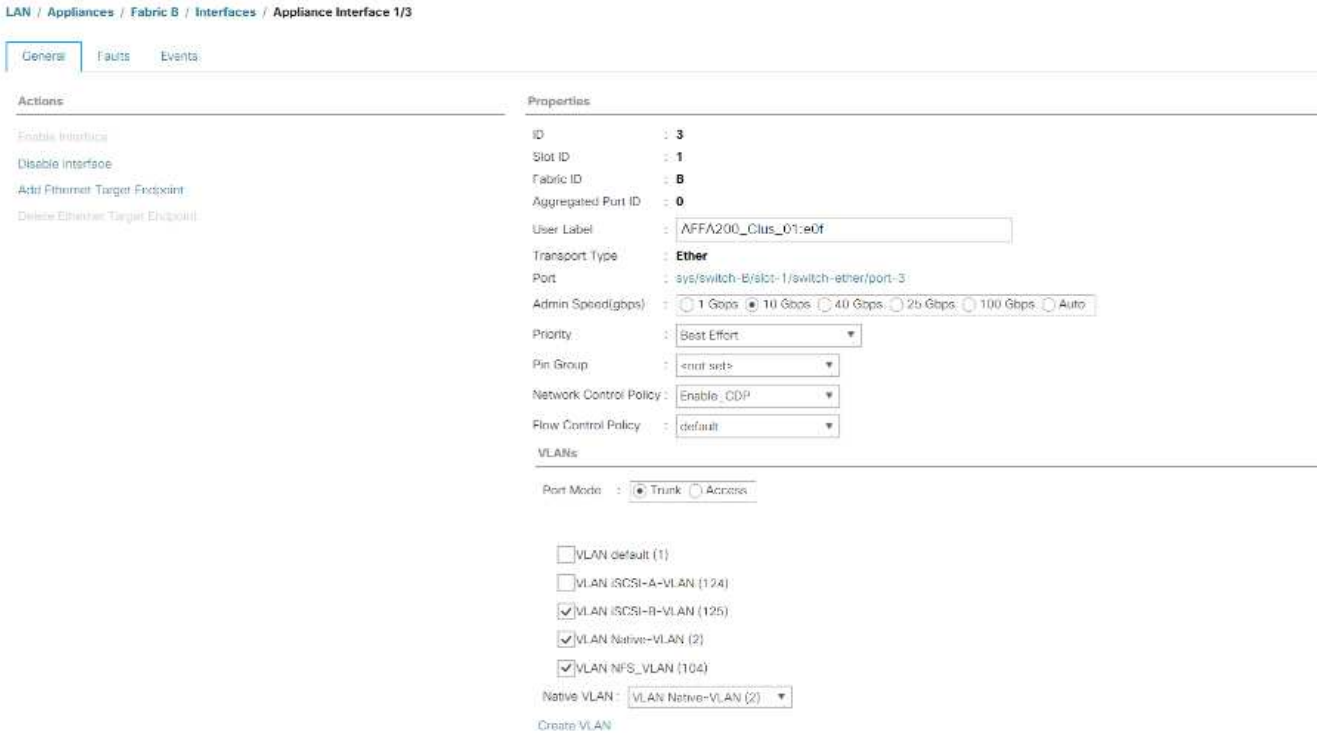


32. 확인 을 클릭한 다음 확인 을 다시 클릭하여 정책을 만듭니다.
33. 탐색 창의 LAN > 어플라이언스 클라우드 에서 Fabric A 트리를 확장합니다.
34. Interfaces를 확장합니다.
35. 어플라이언스 인터페이스 1/3을 선택합니다.
36. User Label 필드에 '<storage_controller_01_name>:e0e'와 같은 스토리지 컨트롤러 포트를 나타내는 정보를 입력합니다. 변경 내용 저장 및 확인 을 클릭합니다.
37. Enable_CDP Network Control Policy를 선택하고 Save Changes and OK를 선택합니다.
38. VLAN에서 iSCSI-A-VLAN, NFS VLAN 및 기본 VLAN을 선택합니다. Native-VLAN을 Native VLAN으로 설정한다. 기본 VLAN 선택을 취소합니다.
39. 변경 내용 저장 및 확인 을 클릭합니다.



40. Fabric A 아래에서 Appliance Interface 1/4를 선택합니다
41. User Label 필드에 '<storage_controller_02_name>:e0e'와 같은 스토리지 컨트롤러 포트를 나타내는 정보를 입력합니다. 변경 내용 저장 및 확인 을 클릭합니다.
42. Enable_CDP Network Control Policy를 선택하고 Save Changes and OK를 선택합니다.
43. VLAN에서 iSCSI-A-VLAN, NFS VLAN 및 기본 VLAN을 선택합니다.
44. Native-VLAN을 Native VLAN으로 설정한다.
45. 기본 VLAN 선택을 취소합니다.
46. 변경 내용 저장 및 확인 을 클릭합니다.
47. 탐색 창의 LAN > 어플라이언스 클라우드 에서 Fabric B 트리를 확장합니다.
48. Interfaces를 확장합니다.
49. 어플라이언스 인터페이스 1/3을 선택합니다.
50. User Label 필드에 '<storage_controller_01_name>:e0f'와 같은 스토리지 컨트롤러 포트를 나타내는 정보를 입력합니다. 변경 내용 저장 및 확인 을 클릭합니다.

51. Enable_CDP Network Control Policy를 선택하고 Save Changes and OK를 선택합니다.
52. VLAN에서 iSCSI-B-VLAN, NFS VLAN 및 기본 VLAN을 선택합니다. Native-VLAN을 Native VLAN으로 설정한다. 기본 VLAN을 선택 취소합니다.

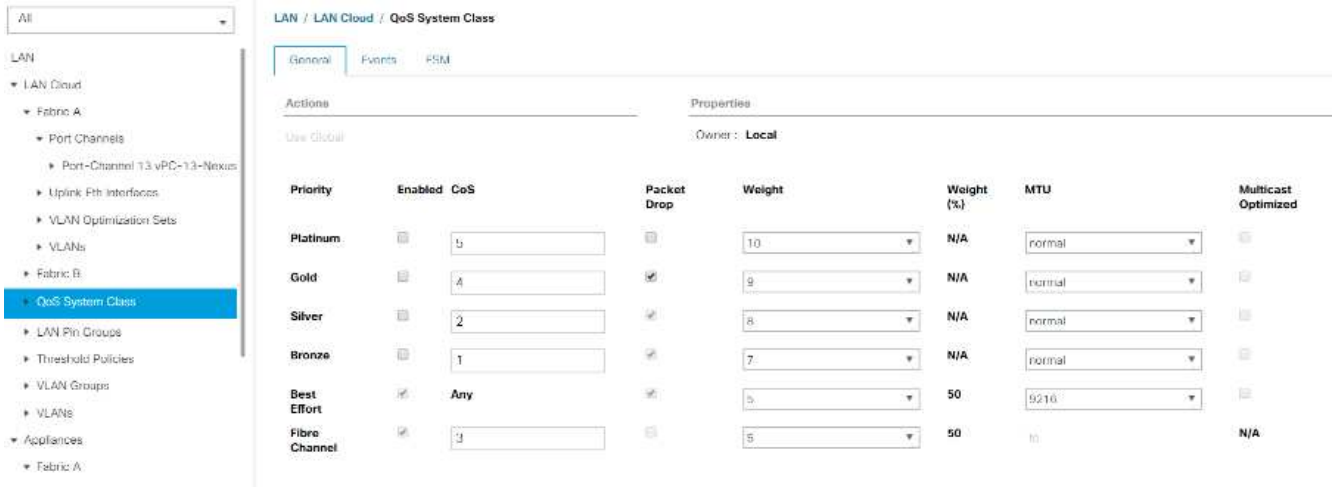


53. 변경 내용 저장 및 확인 을 클릭합니다.
54. Fabric B 아래에서 Appliance Interface 1/4를 선택합니다
55. User Label 필드에 '<storage_controller_02_name>:e0f'와 같은 스토리지 컨트롤러 포트를 나타내는 정보를 입력합니다. 변경 내용 저장 및 확인 을 클릭합니다.
56. Enable_CDP Network Control Policy를 선택하고 Save Changes and OK를 선택합니다.
57. VLAN에서 iSCSI-B-VLAN, NFS VLAN 및 기본 VLAN을 선택합니다. Native-VLAN을 Native VLAN으로 설정한다. 기본 VLAN을 선택 취소합니다.
58. 변경 내용 저장 및 확인 을 클릭합니다.

Cisco UCS 패브릭에서 점보 프레임을 설정합니다

Cisco UCS 패브릭에서 점보 프레임을 구성하고 서비스 품질을 설정하려면 다음 단계를 수행하십시오.

1. Cisco UCS Manager의 탐색 창에서 LAN 탭을 클릭합니다.
2. LAN > LAN Cloud > QoS System Class 를 선택합니다.
3. 오른쪽 창에서 일반 탭을 클릭합니다.
4. Best Effort 행의 MTU 열 아래에 있는 상자에 9216을 입력합니다.



5. 변경 내용 저장 을 클릭합니다.
6. 확인 을 클릭합니다.

Cisco UCS 섀시를 확인합니다

모든 Cisco UCS 섀시를 확인하려면 다음 단계를 수행하십시오.

1. Cisco UCS Manager에서 장비 탭을 선택한 다음 오른쪽의 장비 탭을 확장합니다.
2. 장비 > 섀시를 확장합니다.
3. 섀시 1에 대한 작업에서 섀시 승인 을 선택합니다.
4. 확인을 클릭한 다음 확인을 클릭하여 섀시 확인을 완료합니다.
5. 닫기 를 클릭하여 속성 창을 닫습니다.

Cisco UCS 4.0(1b) 펌웨어 이미지를 로드합니다

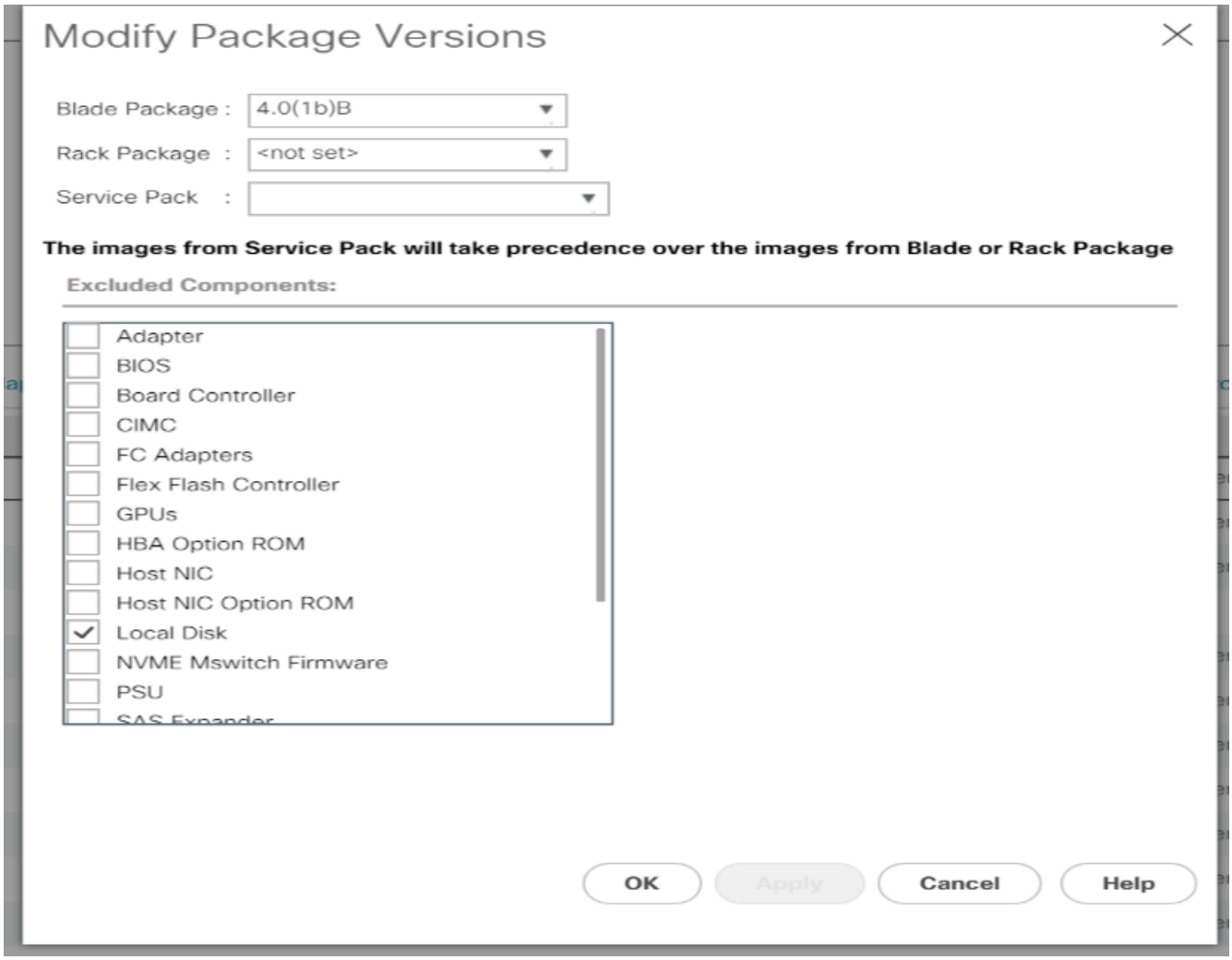
Cisco UCS Manager 소프트웨어 및 Cisco UCS Fabric Interconnect 소프트웨어를 버전 4.0(1b)으로 업그레이드하려면 을 참조하십시오 "Cisco UCS Manager 설치 및 업그레이드 가이드".

호스트 펌웨어 패키지를 생성합니다

관리자는 펌웨어 관리 정책을 사용하여 지정된 서버 구성에 해당하는 패키지를 선택할 수 있습니다. 이러한 정책에는 종종 어댑터, BIOS, 보드 컨트롤러, FC 어댑터, HBA(호스트 버스 어댑터) 옵션 ROM 및 스토리지 컨트롤러 속성에 대한 패키지가 포함됩니다.

Cisco UCS 환경에서 지정된 서버 구성에 대한 펌웨어 관리 정책을 생성하려면 다음 단계를 수행하십시오.

1. Cisco UCS Manager의 경우 왼쪽에 있는 서버 를 클릭합니다.
2. 정책 > 루트를 선택합니다.
3. 호스트 펌웨어 패키지를 확장합니다.
4. 기본값을 선택합니다.
5. 작업 창에서 패키지 버전 수정을 선택합니다.
6. 두 블레이드 패키지 모두에 대해 버전 4.0(1b)을 선택합니다.



7. OK(확인) 를 클릭한 다음 OK(확인) 를 다시 클릭하여 호스트 펌웨어 패키지를 수정합니다.

MAC 주소 풀을 생성합니다

Cisco UCS 환경에 필요한 MAC 주소 풀을 구성하려면 다음 단계를 수행하십시오.

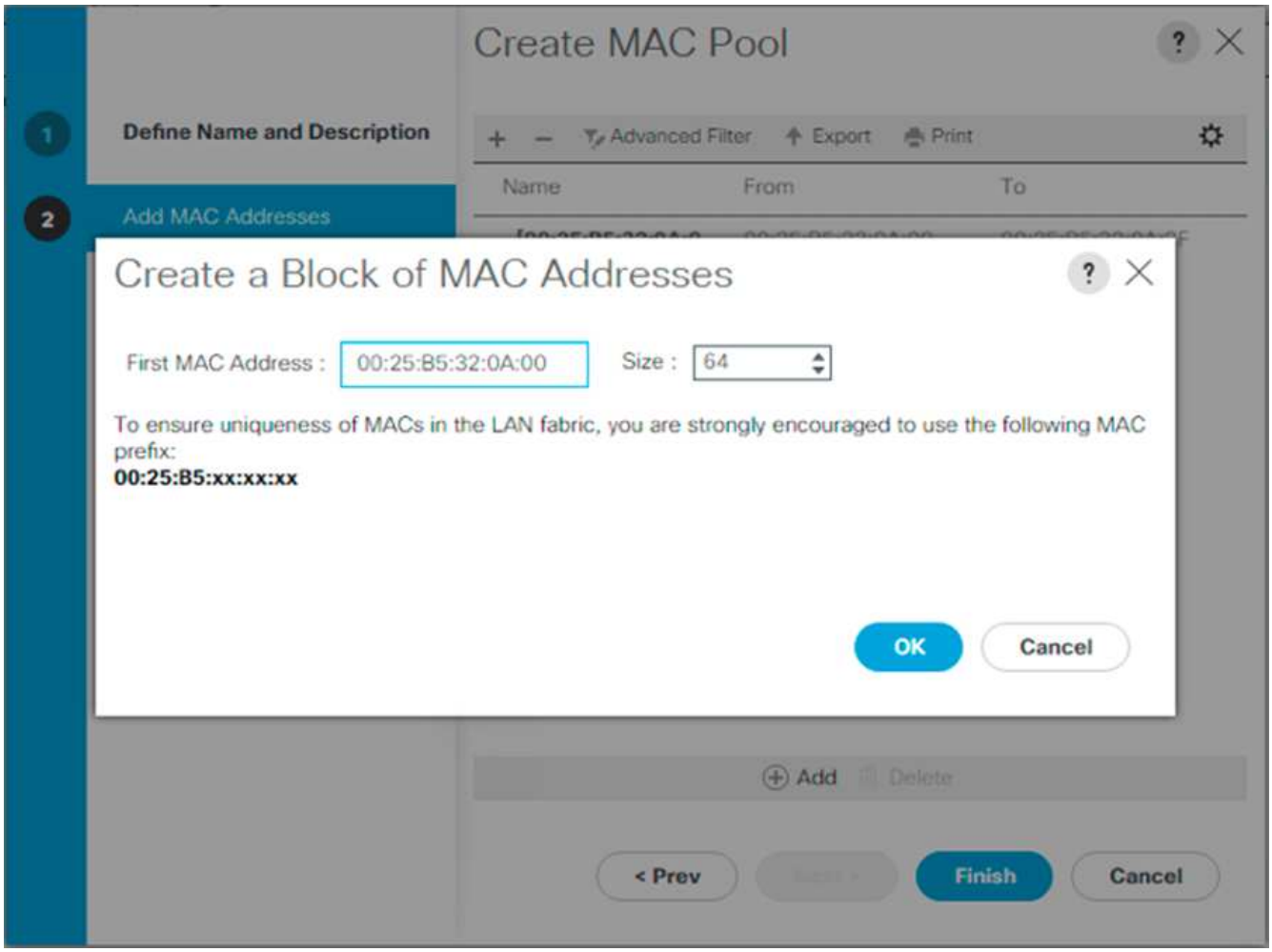
1. Cisco UCS Manager의 경우 왼쪽에 있는 LAN을 클릭합니다.
2. Pools > root 를 선택합니다.

   이 절차에서는 각 스위칭 패브릭에 대해 하나씩 두 개의 MAC 주소 풀이 생성됩니다.

3. 루트 조직 아래에서 MAC Pools 를 마우스 오른쪽 단추로 클릭합니다.
4. MAC 주소 풀을 생성하려면 MAC 풀 생성 을 선택합니다.
5. MAC-Pool-A를 MAC 풀의 이름으로 입력합니다.
6. 선택 사항: MAC 풀에 대한 설명을 입력합니다.
7. 할당 순서 옵션으로 Sequential(순차)을 선택합니다. 다음 을 클릭합니다.
8. 추가 를 클릭합니다.
9. 시작 MAC 주소를 지정합니다.

FlexPod 솔루션의 경우 모든 MAC 주소를 패브릭 A 주소로 식별하기 위해 시작 MAC 주소의 마지막 옥텟에 0A를 배치하는 것이 좋습니다. 이 예에서는 첫 번째 MAC 주소로 00:25:B5:32:0A:00을 제공하는 Cisco UCS 도메인 번호 정보도 포함하는 예를 전달했습니다.

10. 사용 가능한 블레이드 또는 서버 리소스를 지원하기에 충분한 MAC 주소 풀의 크기를 지정합니다. 확인 을 클릭합니다.



11. 마침 을 클릭합니다.
12. 확인 메시지에서 확인 을 클릭합니다.
13. 루트 조직 아래에서 MAC Pools 를 마우스 오른쪽 단추로 클릭합니다.
14. MAC 주소 풀을 생성하려면 MAC 풀 생성 을 선택합니다.
15. MAC-Pool-B를 MAC 풀의 이름으로 입력합니다.
16. 선택 사항: MAC 풀에 대한 설명을 입력합니다.
17. 할당 순서 옵션으로 Sequential(순차)을 선택합니다. 다음 을 클릭합니다.
18. 추가 를 클릭합니다.
19. 시작 MAC 주소를 지정합니다.

FlexPod 솔루션의 경우, 이 풀의 모든 MAC 주소를 패브릭 B 주소로 식별하기 위해 시작 MAC 주소의 마지막 옥텟에 0B를 배치하는 것이 좋습니다. 다시 한 번, 첫 번째 MAC 주소로 00:25:B5:32:0B:00을 제공하는 Cisco UCS 도메인 번호 정보를 포함하는 예를 들어보겠습니다.

20. 사용 가능한 블레이드 또는 서버 리소스를 지원하기에 충분한 MAC 주소 풀의 크기를 지정합니다. 확인 을 클릭합니다.
21. 마침 을 클릭합니다.
22. 확인 메시지에서 확인 을 클릭합니다.

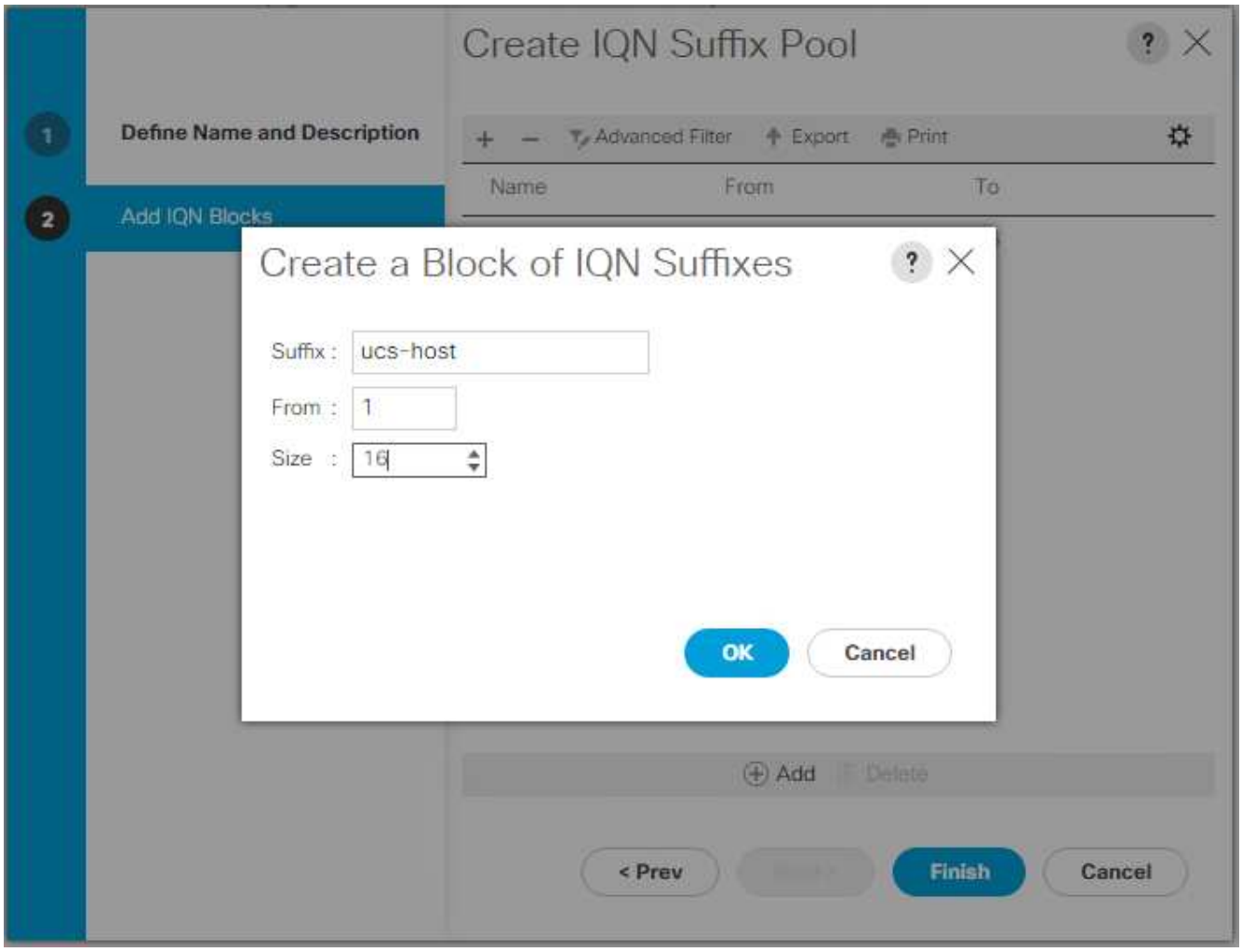
iSCSI IQN 풀을 생성합니다

Cisco UCS 환경에 필요한 IQN 풀을 구성하려면 다음 단계를 수행하십시오.

1. Cisco UCS Manager의 경우 왼쪽에서 SAN을 클릭합니다.
2. Pools > root 를 선택합니다.
3. IQN Pools 를 마우스 오른쪽 버튼으로 클릭합니다.
4. IQN 접미사 풀 생성 을 선택하여 IQN 풀을 생성합니다.
5. IQN 풀의 이름에 IQN-Pool을 입력합니다.
6. 선택 사항: IQN 풀에 대한 설명을 입력합니다.
7. 접두사로 iqn.1992-08.com.cisco` 를 입력합니다.
8. 할당 순서에서 순차적 을 선택합니다. 다음 을 클릭합니다.
9. 추가 를 클릭합니다.
10. 접미사로 UCS-host를 입력합니다.

여러 Cisco UCS 도메인을 사용 중인 경우 보다 구체적인 IQN 접미사를 사용해야 할 수 있습니다.

11. 보낸 사람 필드에 1을 입력합니다.
12. 사용 가능한 서버 리소스를 지원하기에 충분한 IQN 블록 크기를 지정합니다. 확인 을 클릭합니다.



13. 마침 을 클릭합니다.

iSCSI 이니시에이터 **IP** 주소 풀을 생성합니다

Cisco UCS 환경에 필요한 IP 풀 iSCSI 부트를 구성하려면 다음 단계를 수행하십시오.

1. Cisco UCS Manager의 경우 왼쪽에 있는 LAN을 클릭합니다.
2. Pools > root 를 선택합니다.
3. IP Pools 를 마우스 오른쪽 버튼으로 클릭합니다.
4. Create IP Pool 을 선택합니다.
5. IP 풀 이름으로 iSCSI-IP-Pool-A를 입력합니다.
6. 선택 사항: IP 풀에 대한 설명을 입력합니다.
7. 할당 순서에 대해 Sequential(순차) 을 선택합니다. 다음 을 클릭합니다.
8. 추가 를 클릭하여 IP 주소 블록을 추가합니다.
9. From(보낸 사람) 필드에 iSCSI IP 주소로 할당할 범위의 시작 부분을 입력합니다.
10. 서버 수용 가능한 주소 크기로 설정합니다. 확인 을 클릭합니다.
11. 다음 을 클릭합니다.

12. 마침 을 클릭합니다.
13. IP Pools 를 마우스 오른쪽 버튼으로 클릭합니다.
14. Create IP Pool 을 선택합니다.
15. IP 풀 이름으로 iSCSI-IP-Pool-B를 입력합니다.
16. 선택 사항: IP 풀에 대한 설명을 입력합니다.
17. 할당 순서에 대해 Sequential(순차) 을 선택합니다. 다음 을 클릭합니다.
18. 추가 를 클릭하여 IP 주소 블록을 추가합니다.
19. From(보낸 사람) 필드에 iSCSI IP 주소로 할당할 범위의 시작 부분을 입력합니다.
20. 서버 수용 가능한 주소 크기로 설정합니다. 확인 을 클릭합니다.
21. 다음 을 클릭합니다.
22. 마침 을 클릭합니다.

UUID 접미사 풀을 생성합니다

Cisco UCS 환경에 필요한 UUID(Universally Unique Identifier) 접미사 풀을 구성하려면 다음 단계를 완료하십시오.

1. Cisco UCS Manager의 경우 왼쪽에 있는 서버 를 클릭합니다.
2. Pools > root 를 선택합니다.
3. UUID 접미사 풀 을 마우스 오른쪽 버튼으로 클릭합니다.
4. UUID 접미사 풀 생성 을 선택합니다.
5. UUID 접미사 풀의 이름으로 UUID-Pool을 입력합니다.
6. 선택 사항: UUID 접미사 풀에 대한 설명을 입력합니다.
7. 원본에 구속되는 옵션에서 접두어를 유지합니다.
8. 할당 순서에 대해 Sequential(순차) 을 선택합니다.
9. 다음 을 클릭합니다.
10. 추가 를 클릭하여 UUID 블록을 추가합니다.
11. 보낸 사람 필드를 기본 설정으로 유지합니다.
12. 사용 가능한 블레이드 또는 서버 리소스를 지원하기에 충분한 UUID 블록의 크기를 지정합니다. 확인 을 클릭합니다.
13. 마침 을 클릭합니다.
14. 확인 을 클릭합니다.

서버 풀을 생성합니다

Cisco UCS 환경에 필요한 서버 풀을 구성하려면 다음 단계를 수행하십시오.

사용자 환경에 필요한 세분화 수준을 달성하려면 고유한 서버 풀을 생성하는 것이 좋습니다.

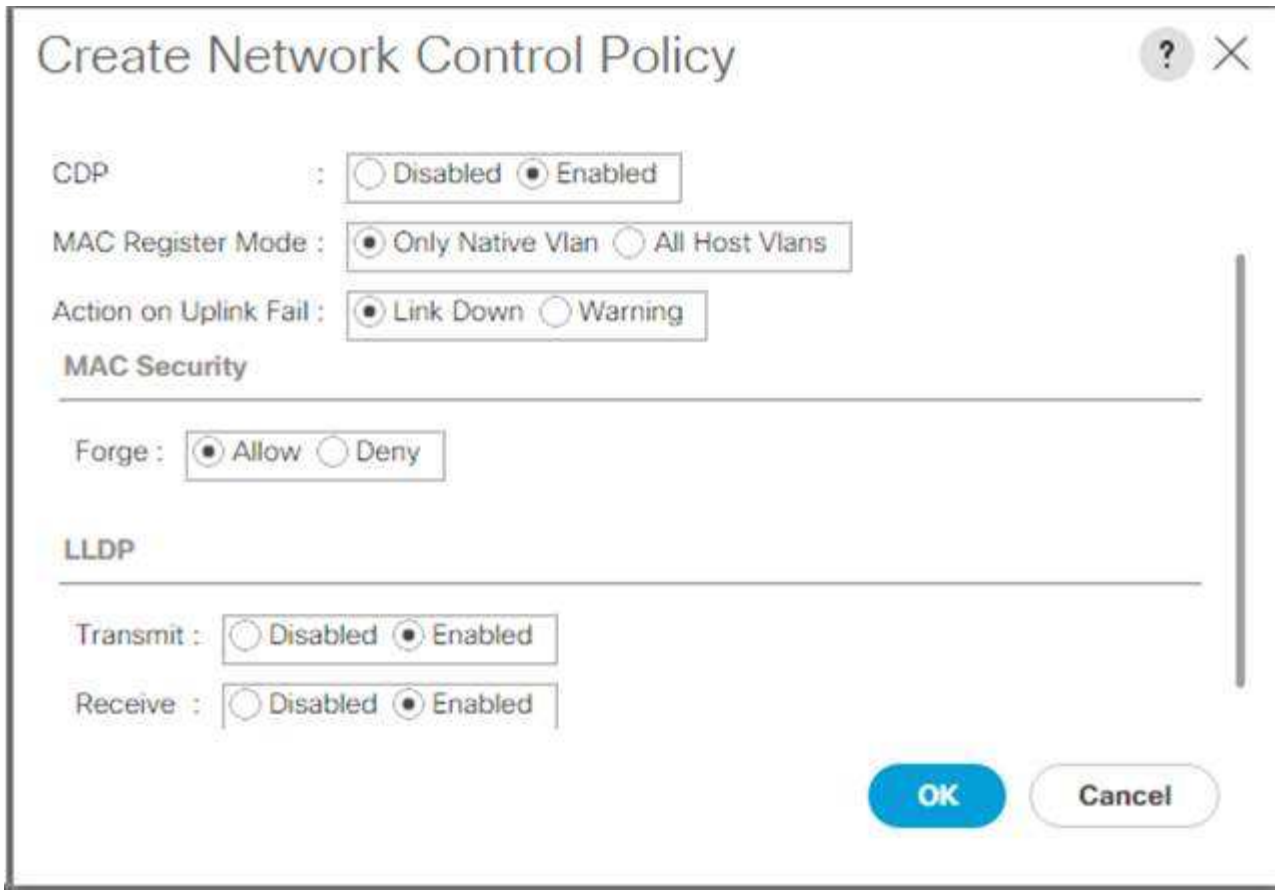
1. Cisco UCS Manager의 경우 왼쪽에 있는 서버 를 클릭합니다.
2. Pools > root 를 선택합니다.

3. 서버 풀 을 마우스 오른쪽 단추로 클릭합니다.
4. Create Server Pool 을 선택합니다.
5. 서버 풀의 이름으로 Infra-Pool을 입력합니다.
6. 선택 사항: 서버 풀에 대한 설명을 입력합니다. 다음 을 클릭합니다.
7. VMware 관리 클러스터에 사용할 서버를 두 개 이상 선택하고 >> 를 클릭하여 Infra-Pool의 서버 풀에 추가합니다.
8. 마침 을 클릭합니다.
9. 확인 을 클릭합니다.

Cisco Discovery Protocol 및 Link Layer Discovery Protocol에 대한 네트워크 제어 정책을 생성합니다

CDP(Cisco Discovery Protocol) 및 LLDP(Link Layer Discovery Protocol)에 대한 네트워크 제어 정책을 만들려면 다음 단계를 수행하십시오.

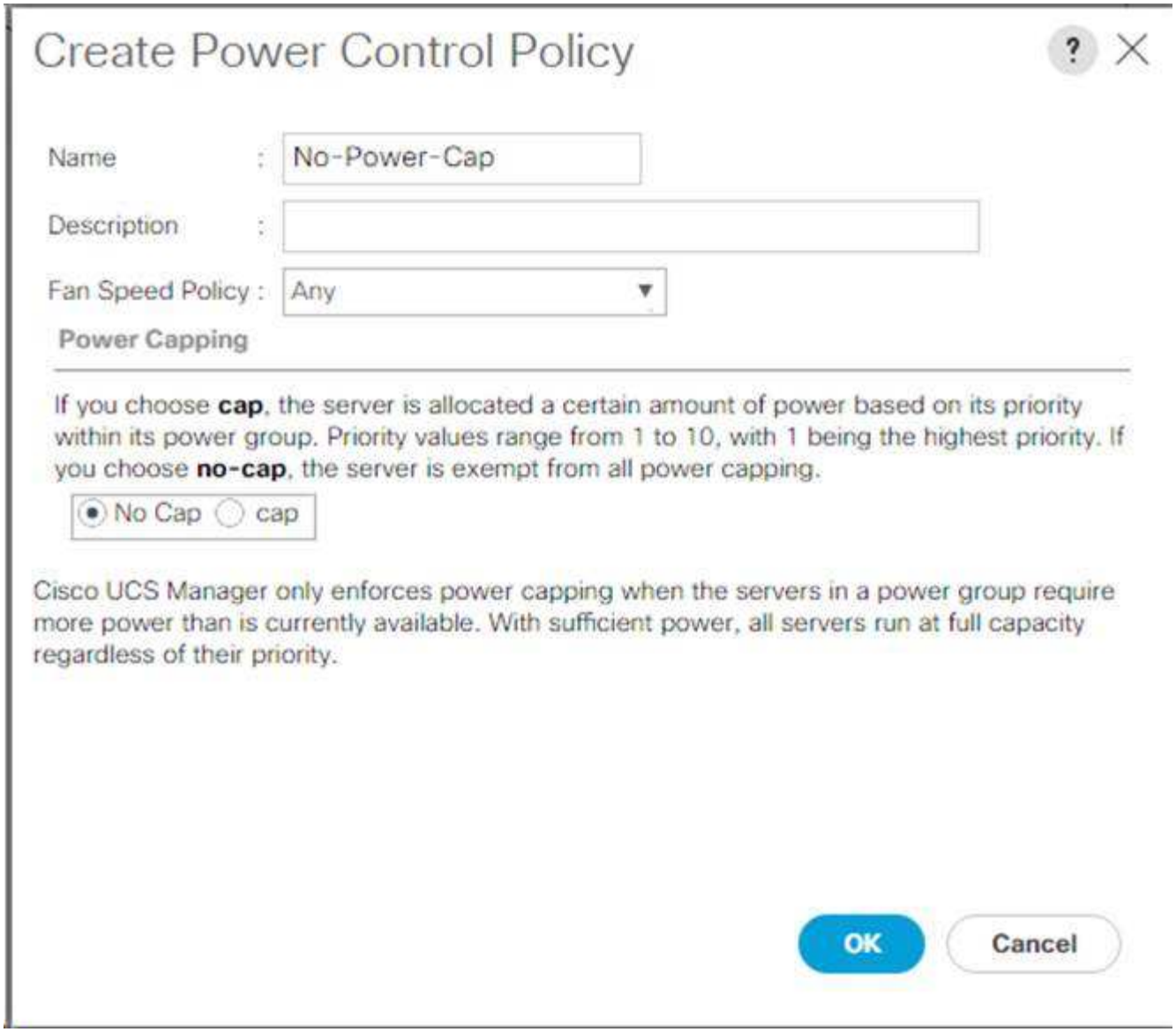
1. Cisco UCS Manager의 경우 왼쪽에 있는 LAN을 클릭합니다.
2. 정책 > 루트를 선택합니다.
3. 네트워크 제어 정책 을 마우스 오른쪽 단추로 클릭합니다.
4. 네트워크 제어 정책 생성 을 선택합니다.
5. Enable-CDP-LLDP 정책 이름을 입력합니다.
6. CDP의 경우 사용 옵션을 선택합니다.
7. LLDP의 경우 아래로 스크롤하여 전송 및 수신 모두에 대해 사용 을 선택합니다.
8. 확인 을 클릭하여 네트워크 제어 정책을 생성합니다. 확인 을 클릭합니다.



전원 제어 정책을 생성합니다

Cisco UCS 환경에 대한 전원 제어 정책을 생성하려면 다음 단계를 수행하십시오.

1. Cisco UCS Manager의 경우 왼쪽에서 서버 탭을 클릭합니다.
2. 정책 > 루트를 선택합니다.
3. 전원 제어 정책 을 마우스 오른쪽 단추로 클릭합니다.
4. 전원 제어 정책 생성 을 선택합니다.
5. 전원 제어 정책 이름으로 No-Power-Cap을 입력합니다.
6. 전력 제한 설정을 캡 없음 으로 변경합니다.
7. 확인 을 클릭하여 전원 제어 정책을 만듭니다. 확인 을 클릭합니다.



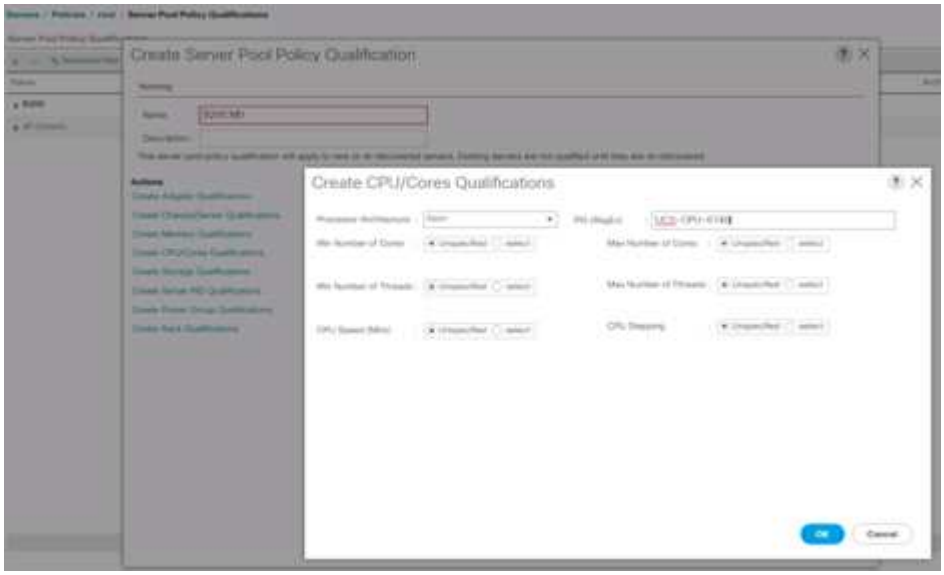
서버 풀 검증 정책 생성(선택 사항)

Cisco UCS 환경에 대해 선택적인 서버 풀 검증 정책을 생성하려면 다음 단계를 완료하십시오.

이 예에서는 Intel E2660 v4 Xeon Broadwell 프로세서를 사용하는 Cisco UCS B-Series 서버에 대한 정책을 생성합니다.

1. Cisco UCS Manager의 경우 왼쪽에 있는 서버 를 클릭합니다.
2. 정책 > 루트를 선택합니다.
3. 서버 풀 정책 자격 을 선택합니다.
4. Create Server Pool Policy Qualification 또는 Add를 선택합니다.
5. 정책 이름을 인텔 으로 지정합니다.
6. Create CPU/Cores Qualifications(CPU/코어 자격 생성) 를 선택합니다.
7. 프로세서/아키텍처로 제온을 선택합니다.

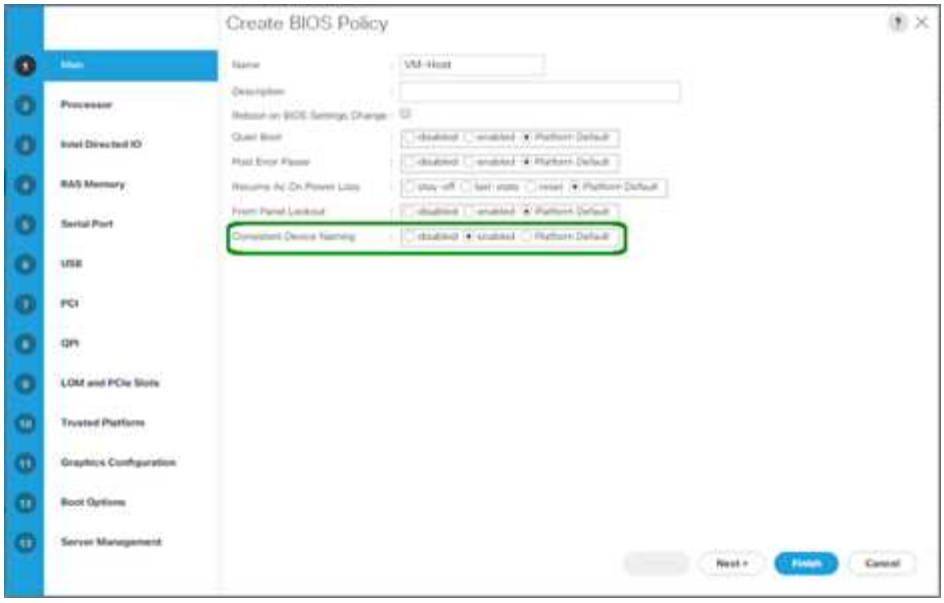
8. 프로세스 ID(PID)로 '<UCS-CPU-PID>'를 입력합니다.
9. 확인 을 클릭하여 CPU/코어 조건을 만듭니다.
10. 확인 을 클릭하여 정책을 생성한 다음 확인 을 클릭합니다.



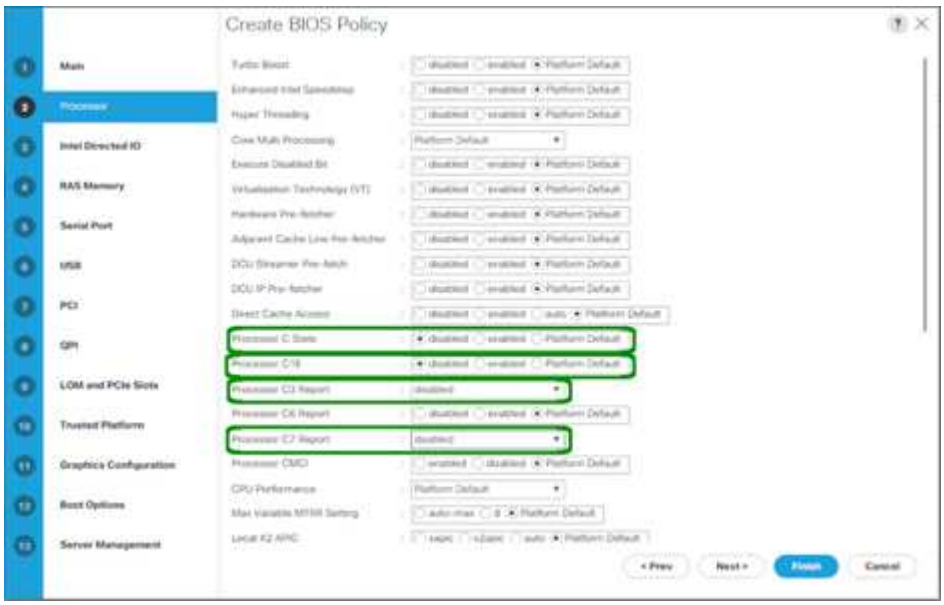
서버 **BIOS** 정책을 만듭니다

Cisco UCS 환경에 대한 서버 BIOS 정책을 생성하려면 다음 단계를 수행하십시오.

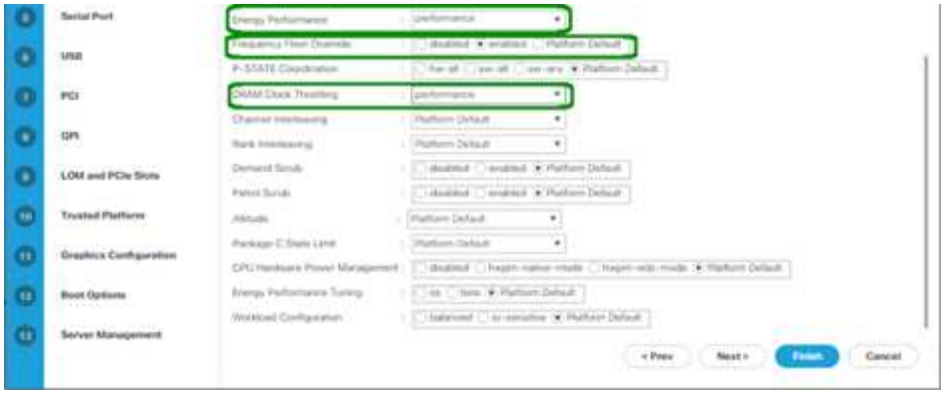
1. Cisco UCS Manager의 경우 왼쪽에 있는 서버 를 클릭합니다.
2. 정책 > 루트를 선택합니다.
3. BIOS 정책을 마우스 오른쪽 단추로 클릭합니다.
4. BIOS 정책 생성 을 선택합니다.
5. BIOS 정책 이름으로 VM-Host를 입력합니다.
6. 자동 부팅 설정을 사용 안 함으로 변경합니다.
7. 정합성 보장 장치 이름을 사용으로 변경합니다.



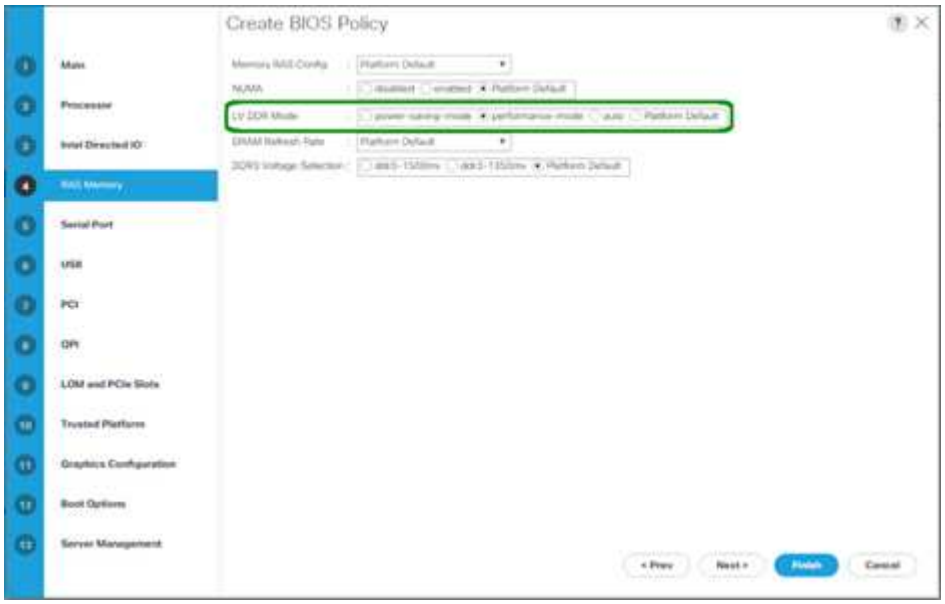
8. 프로세서 탭을 선택하고 다음 매개 변수를 설정합니다.
   - 프로세서 C 상태: 비활성화됨
   - 처리기 C1E: 비활성화
   - 프로세서 C3 보고서: 사용 안 함
   - 프로세서 C7 보고서: 사용 안 함



9. 나머지 프로세서 옵션까지 아래로 스크롤하여 다음 매개변수를 설정합니다.
   - 에너지 성능: 성능
   - Frequency Floor Override: enabled(주파수 플로어 재설정
   - DRAM 클럭 제한: 성능



10. RAS 메모리 를 클릭하고 다음 매개변수를 설정합니다.
    - LV DDR 모드: 성능 모드

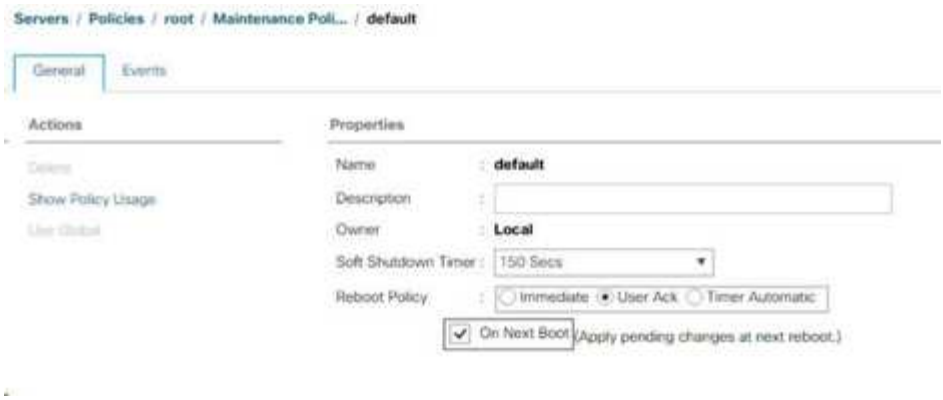


11. 마침 을 클릭하여 BIOS 정책을 만듭니다.
12. 확인 을 클릭합니다.

기본 유지 관리 정책을 업데이트합니다

기본 유지 관리 정책을 업데이트하려면 다음 단계를 완료하십시오.

1. Cisco UCS Manager의 경우 왼쪽에 있는 서버 를 클릭합니다.
2. 정책 > 루트를 선택합니다.
3. Maintenance Policies > default 를 선택합니다.
4. 재부팅 정책을 사용자 승인 으로 변경합니다.
5. 다음 부팅 시 를 선택하여 유지 관리 창을 서버 관리자에게 위임합니다.



6. 변경 내용 저장 을 클릭합니다.
7. 확인 을 클릭하여 변경 사항을 적용합니다.

vNIC 템플릿을 생성합니다

Cisco UCS 환경에 대한 vNIC(Virtual Network Interface Card) 템플릿을 여러 개 생성하려면 이 섹션에 설명된 절차를 완료하십시오.

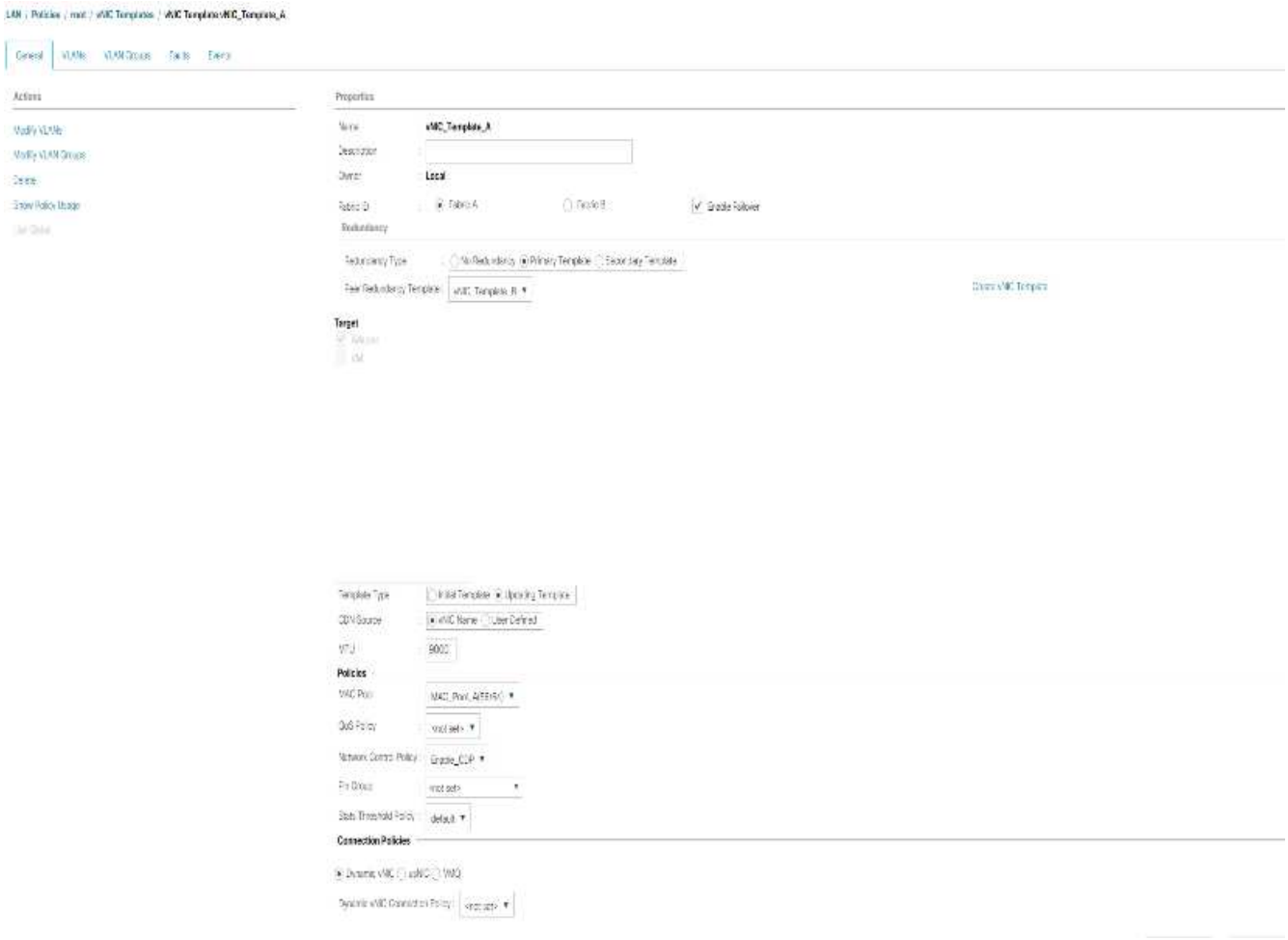
총 4개의 vNIC 템플릿이 생성됩니다.

인프라 **vNIC**를 생성합니다

인프라 vNIC를 생성하려면 다음 단계를 수행하십시오.

1. Cisco UCS Manager의 경우 왼쪽에 있는 LAN을 클릭합니다.
2. 정책 > 루트를 선택합니다.
3. vNIC 템플릿을 마우스 오른쪽 버튼으로 클릭합니다.
4. vNIC 템플릿 생성 을 선택합니다.
5. vNIC 템플릿 이름으로 Site-XX-vNIC_A를 입력합니다.
6. 템플릿 유형으로 Update-template(업데이트-템플릿) 을 선택합니다.
7. Fabric ID로 Fabric A를 선택합니다
8. Enable Failover 옵션이 선택되지 않았는지 확인합니다.
9. 중복 유형으로 기본 템플릿을 선택합니다.
10. 피어 중복 템플릿은 "<설정되지 않음>"으로 설정된 상태로 둡니다.
11. 대상에서 어댑터 옵션만 선택되어 있는지 확인합니다.
12. Native-VLAN을 native VLAN으로 설정한다.
13. CDN 소스로 vNIC 이름 을 선택합니다.
14. MTU의 경우 9000을 입력합니다.
15. 허용된 VLAN에서 'Native-VLAN, Site-XX-IB-MGMT, Site-XX-NFS, Site-XX-VM-Traffic'을 선택합니다. 및 Site-XX-vMotion을 참조하십시오. Ctrl 키를 사용하여 이 항목을 여러 개 선택합니다.
16. 선택 을 클릭합니다. 이제 이러한 VLAN이 선택한 VLAN 아래에 나타납니다.

17. MAC Pool 목록에서 MAC_Pool_A를 선택합니다.
18. 네트워크 제어 정책 목록에서 Pool-A를 선택합니다
19. 네트워크 제어 정책 목록에서 Enable-CDP-LLDP 를 선택합니다.
20. 확인 을 클릭하여 vNIC 템플릿을 생성합니다.
21. 확인 을 클릭합니다.

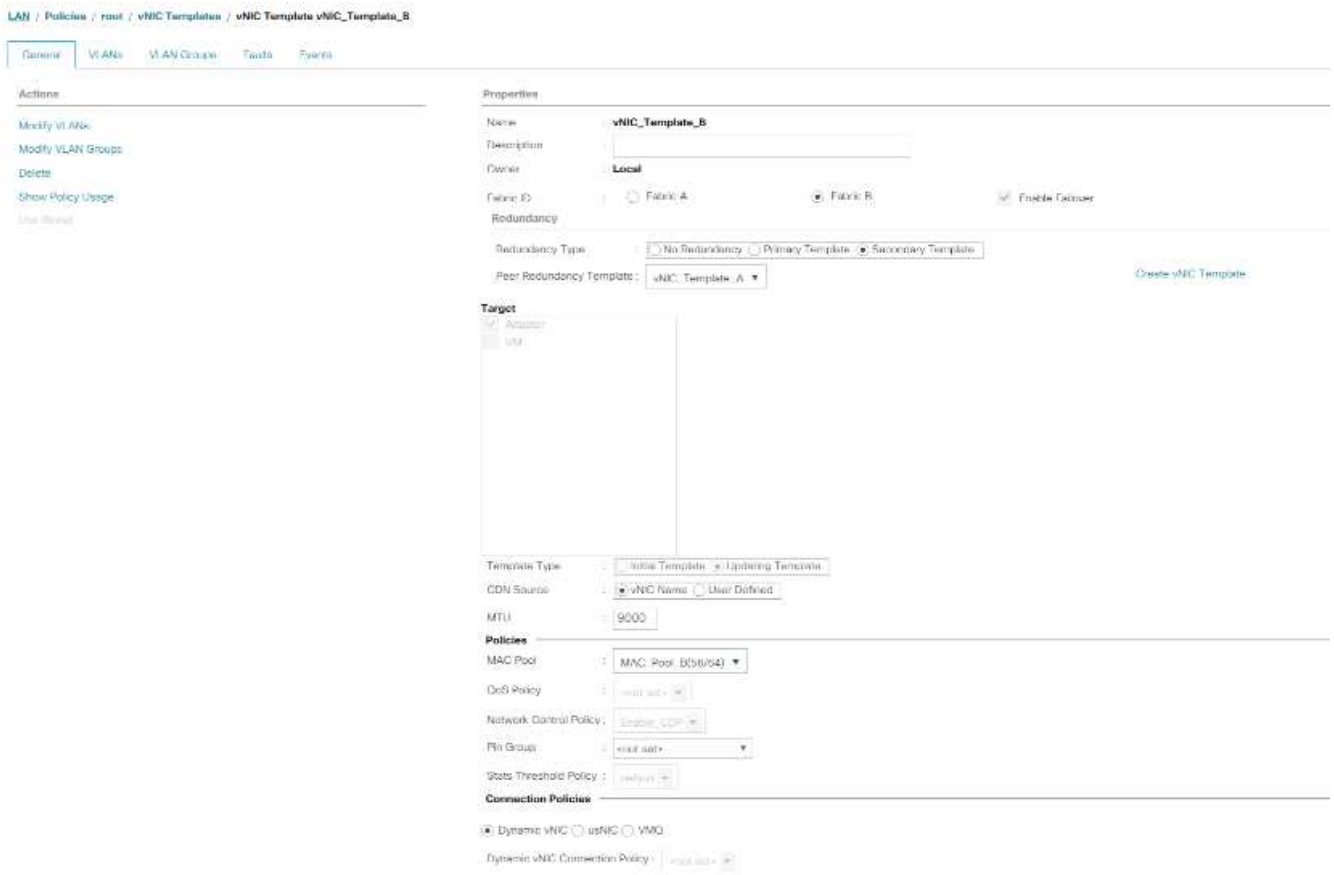


보조 중복 템플릿 Infra-B를 생성하려면 다음 단계를 수행하십시오.

1. Cisco UCS Manager의 경우 왼쪽에 있는 LAN을 클릭합니다.
2. 정책 > 루트를 선택합니다.
3. vNIC 템플릿을 마우스 오른쪽 버튼으로 클릭합니다.
4. vNIC 템플릿 생성 을 선택합니다.
5. vNIC 템플릿 이름으로 Site-XX-vNIC_B를 입력합니다.
6. 템플릿 유형으로 Update-template(업데이트-템플릿) 을 선택합니다.
7. Fabric ID로 Fabric B를 선택합니다
8. Enable Failover 옵션을 선택합니다.

페일오버를 선택하는 것은 하드웨어 레벨에서 이를 처리하고 가상 스위치에서 NIC 장애가 감지되지 않을 가능성을 방지함으로써 링크 페일오버 시간을 개선하는 중요한 단계입니다.

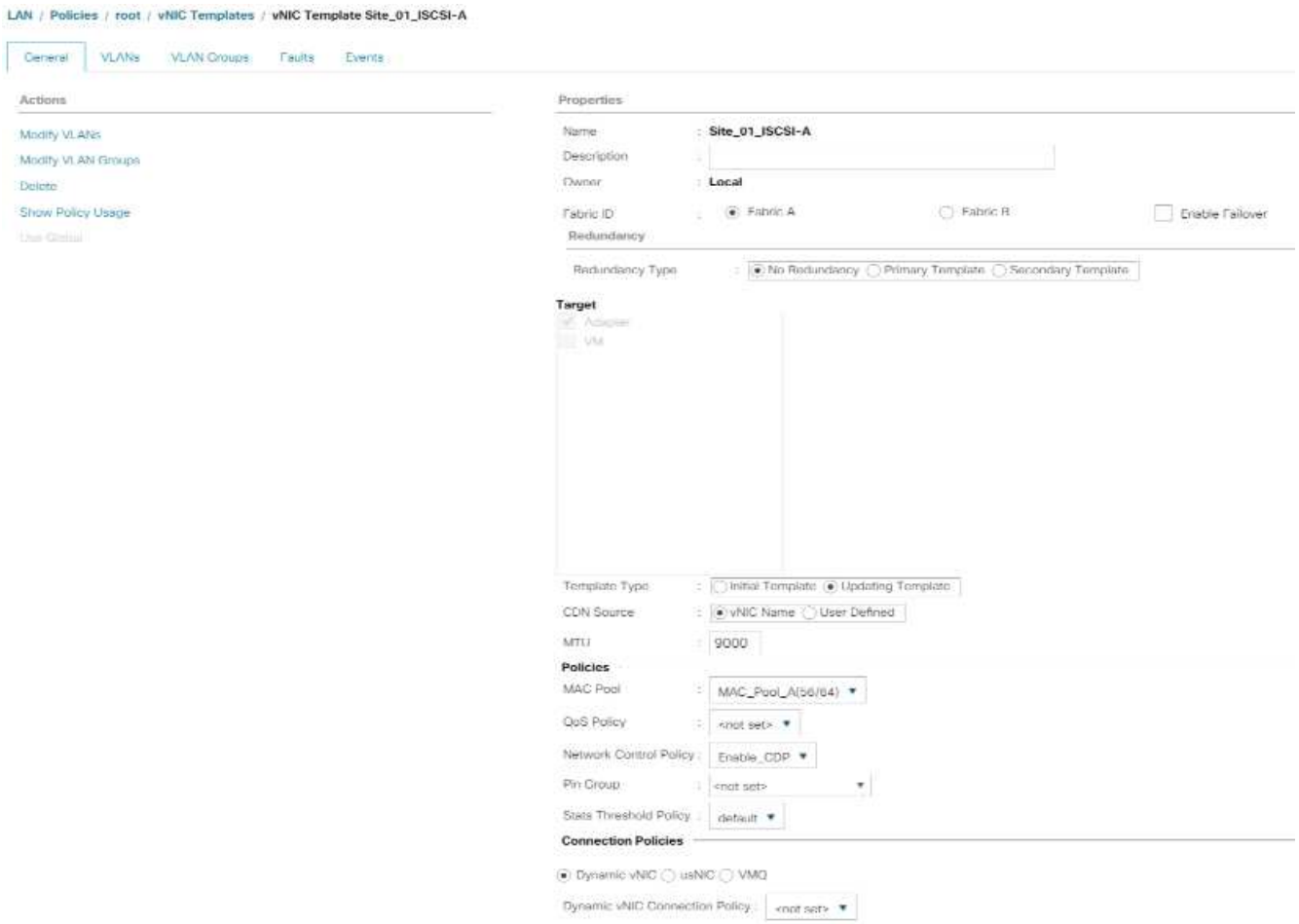
9. 중복 유형으로 기본 템플릿을 선택합니다.
10. 피어 이중화 템플릿은 "vNIC_Template_A"로 설정된 상태로 둡니다.
11. 대상에서 어댑터 옵션만 선택되어 있는지 확인합니다.
12. Native-VLAN을 native VLAN으로 설정한다.
13. CDN 소스로 vNIC 이름 을 선택합니다.
14. MTU의 경우 '9000'을 입력합니다.
15. 허용된 VLAN에서 'Native-VLAN, Site-XX-IB-MGMT, Site-XX-NFS, Site-XX-VM-Traffic'을 선택합니다. 및 Site-XX-vMotion을 참조하십시오. Ctrl 키를 사용하여 이 항목을 여러 개 선택합니다.
16. 선택 을 클릭합니다. 이제 이러한 VLAN이 선택한 VLAN 아래에 나타납니다.
17. MAC Pool 목록에서 MAC_Pool_B를 선택합니다.
18. 네트워크 제어 정책 목록에서 Pool-B를 선택합니다
19. 네트워크 제어 정책 목록에서 Enable-CDP-LLDP 를 선택합니다.
20. 확인 을 클릭하여 vNIC 템플릿을 생성합니다.
21. 확인 을 클릭합니다.



iSCSI vNIC를 생성합니다

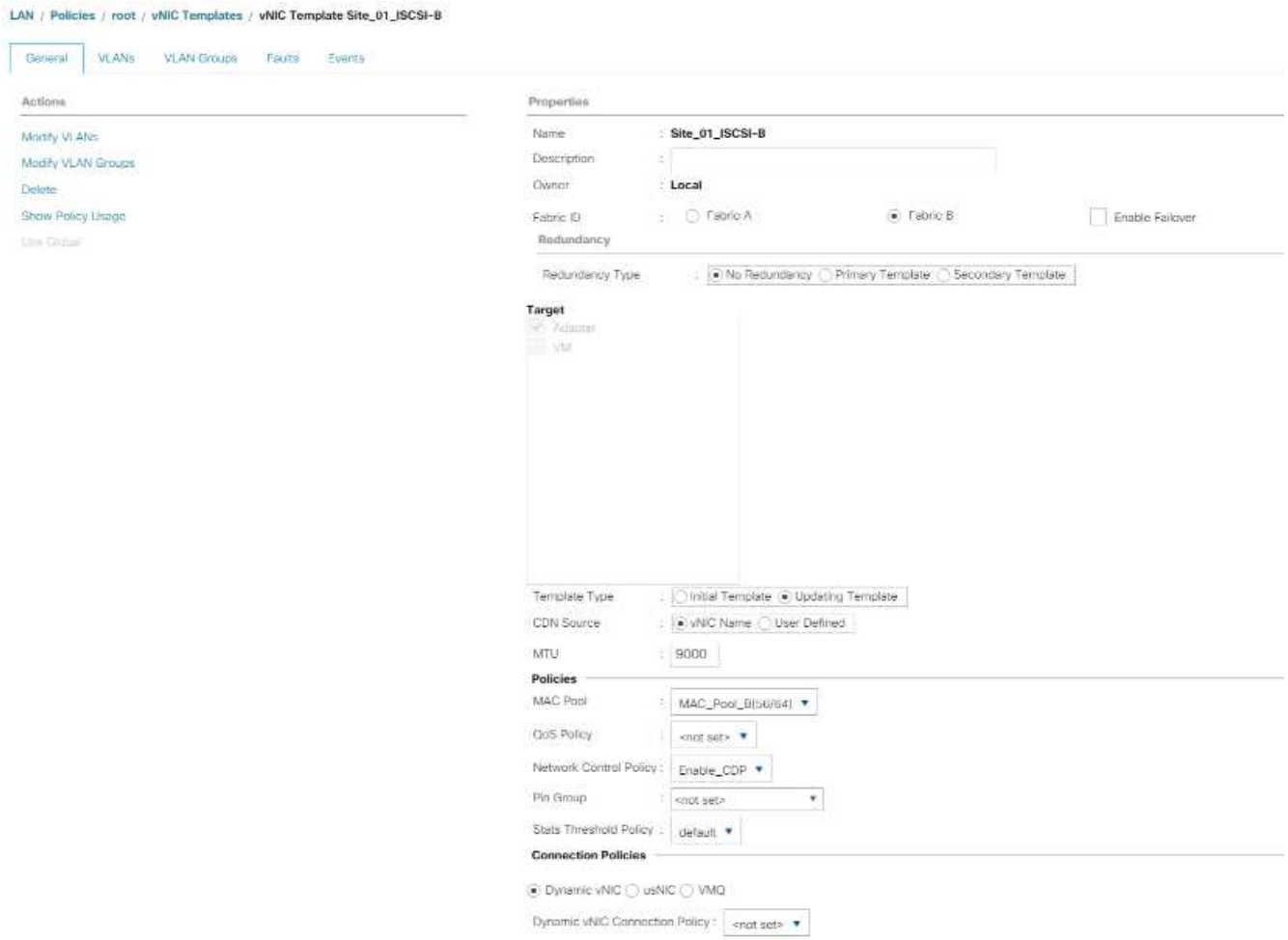
iSCSI vNIC를 생성하려면 다음 단계를 수행하십시오.

1. 왼쪽에서 LAN 을 선택합니다.
2. 정책 > 루트를 선택합니다.
3. vNIC 템플릿을 마우스 오른쪽 버튼으로 클릭합니다.
4. vNIC 템플릿 생성 을 선택합니다.
5. vNIC 템플릿 이름으로 Site-01-iscsi_a를 입력합니다.
6. 패브릭 A 를 선택합니다 Enable Failover 옵션을 선택하지 마십시오.
7. 중복성 유형을 중복되지 않음 으로 설정합니다.
8. 대상에서 어댑터 옵션만 선택되어 있는지 확인합니다.
9. 템플릿 유형으로 템플릿 업데이트를 선택합니다.
10. VLAN에서 Site-01-iSCSI_A_VLAN만 선택합니다.
11. Site-01-iscsi_a_vlan을 기본 VLAN으로 선택합니다.
12. CDN 소스에 대해 vNIC 이름을 설정된 상태로 둡니다.
13. MTU에서 9000을 입력합니다.
14. MAC Pool 목록에서 MAC-Pool-A를 선택합니다
15. 네트워크 제어 정책 목록에서 Enable-CDP-LLDP 를 선택합니다.
16. 확인 을 클릭하여 vNIC 템플릿 생성을 완료합니다.
17. 확인 을 클릭합니다.



18. 왼쪽에서 LAN 을 선택합니다.
19. 정책 > 루트를 선택합니다.
20. vNIC 템플릿을 마우스 오른쪽 버튼으로 클릭합니다.
21. vNIC 템플릿 생성 을 선택합니다.
22. vNIC 템플릿 이름으로 Site-01-ISCSI_B를 입력합니다.
23. Fabric B를 선택합니다 Enable Failover 옵션을 선택하지 마십시오.
24. 중복성 유형을 중복되지 않음 으로 설정합니다.
25. 대상에서 어댑터 옵션만 선택되어 있는지 확인합니다.
26. 템플릿 유형으로 템플릿 업데이트를 선택합니다.
27. VLAN에서 'ite-01-iscsi_B_vlan'만 선택합니다.
28. 네이티브 VLAN으로 Site-01-ISCSI_B_VLAN을 선택한다.
29. CDN 소스에 대해 vNIC 이름을 설정된 상태로 둡니다.
30. MTU에서 9000을 입력합니다.
31. MAC Pool 목록에서 MAC-Pool-B를 선택합니다.
32. Network Control Policy 목록에서 Enable-CDP-LLDP를 선택합니다.
33. 확인 을 클릭하여 vNIC 템플릿 생성을 완료합니다.

34. 확인 을 클릭합니다.



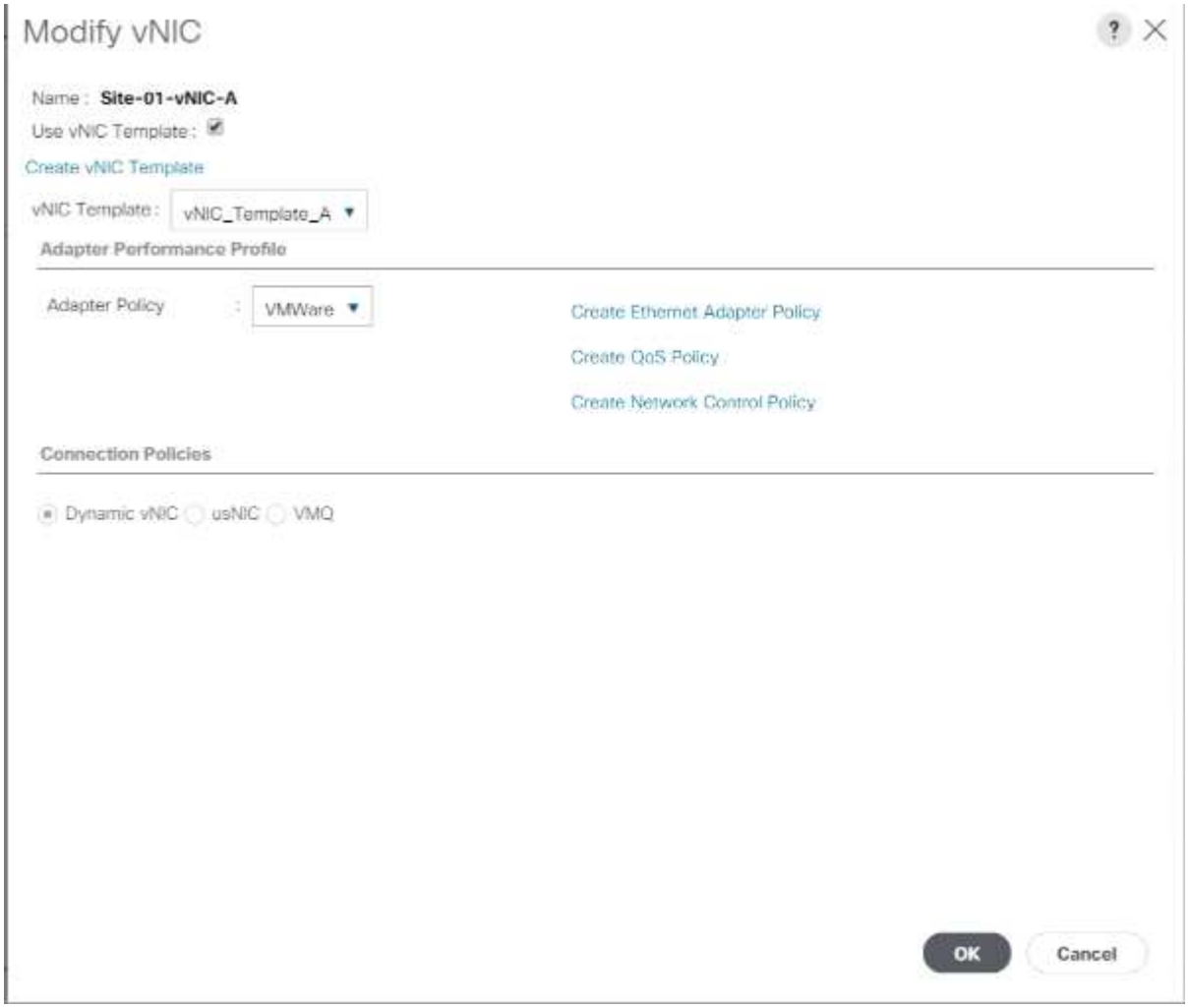
iSCSI 부트에 대한 **LAN** 연결 정책을 생성합니다

이 절차는 두 개의 iSCSI LIF가 클러스터 노드 1('iSCSI_liff 01a' 및 'iscsi_liff 01b')에 있고 두 개의 iSCSI LIF가 클러스터 노드 2('iscsi_liff 02a' 및 'iscsi_liff')에 있는 Cisco UCS 환경에 적용됩니다. 또한, LIF가 패브릭 A(Cisco UCS 6324 A)에 연결되고 B LIF가 패브릭 B(Cisco UCS 6324 B)에 연결된 것으로 가정합니다.

필요한 인프라 LAN 연결 정책을 구성하려면 다음 단계를 수행하십시오.

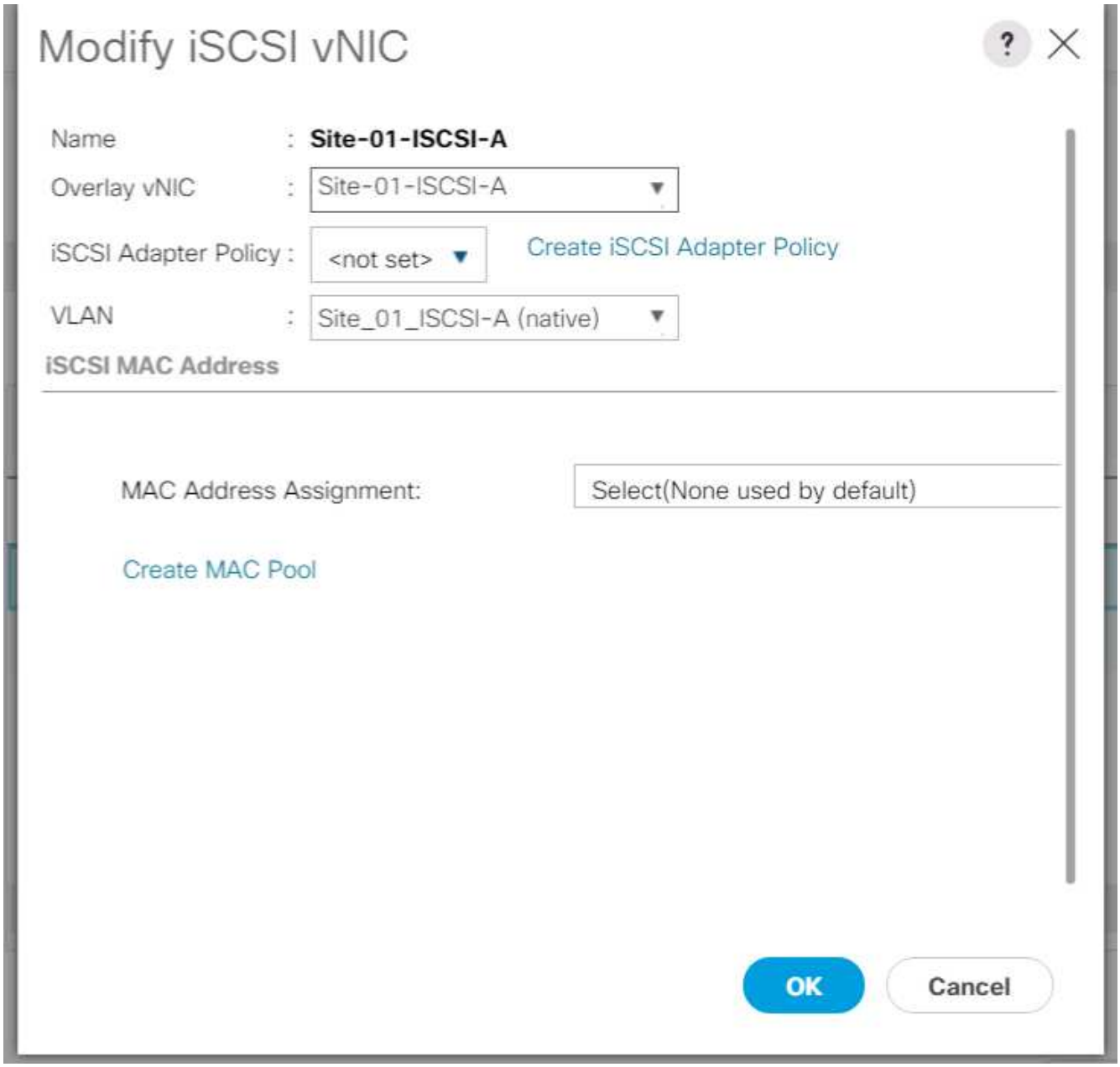
1. Cisco UCS Manager의 경우 왼쪽에 있는 LAN을 클릭합니다.
2. LAN > 정책 > 루트를 선택합니다.
3. LAN 연결 정책을 마우스 오른쪽 단추로 클릭합니다.
4. LAN 연결 정책 생성 을 선택합니다.
5. 정책 이름으로 사이트 XX-Fabric-A를 입력합니다.
6. vNIC를 추가하려면 상단 추가 옵션을 클릭합니다.
7. vNIC 생성 대화 상자에서 vNIC 이름으로 'ite-01-vNIC-A'를 입력합니다.
8. vNIC 템플릿 사용 옵션을 선택합니다.

9. vNIC 템플릿 목록에서 'vNIC_Template_A'를 선택합니다.
10. 어댑터 정책 드롭다운 목록에서 VMware 를 선택합니다.
11. 확인 을 클릭하여 이 vNIC를 정책에 추가합니다.

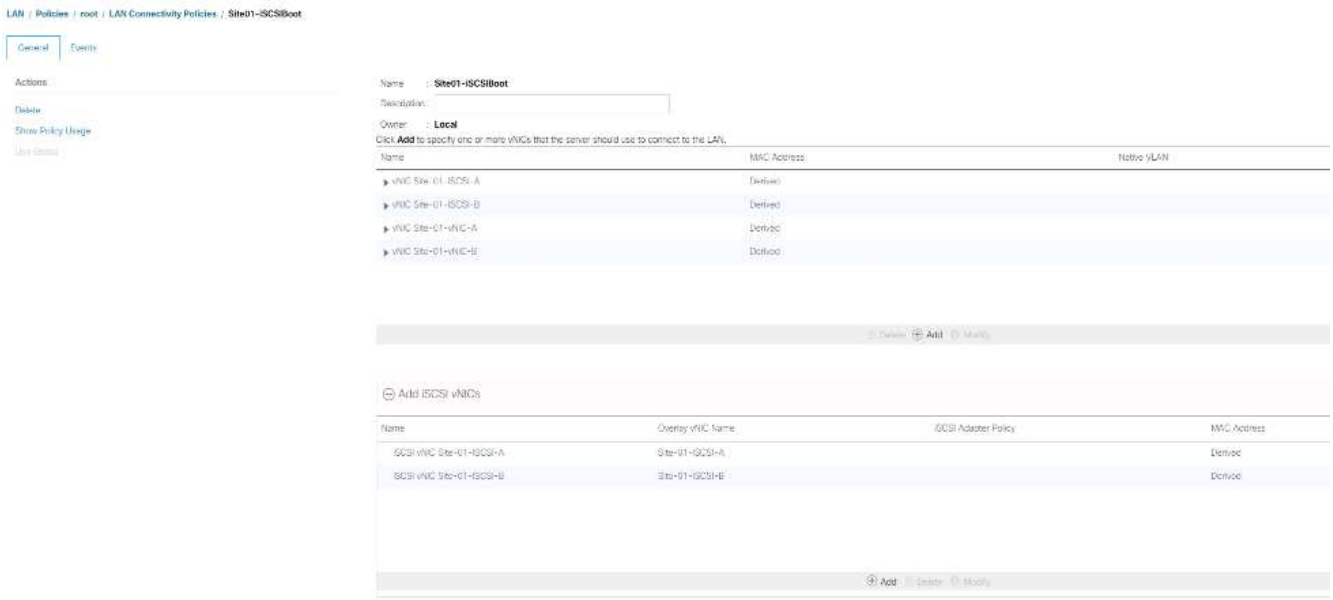


12. vNIC를 추가하려면 상단 추가 옵션을 클릭합니다.
13. vNIC 생성 대화 상자에서 vNIC 이름으로 'ite-01-vNIC-B'를 입력합니다.
14. vNIC 템플릿 사용 옵션을 선택합니다.
15. vNIC 템플릿 목록에서 'vNIC_Template_B'를 선택합니다.
16. 어댑터 정책 드롭다운 목록에서 VMware 를 선택합니다.
17. 확인 을 클릭하여 이 vNIC를 정책에 추가합니다.
18. vNIC를 추가하려면 상단 추가 옵션을 클릭합니다.
19. vNIC 생성 대화 상자에서 vNIC 이름으로 Site-01-iscsi-A를 입력합니다.
20. vNIC 템플릿 사용 옵션을 선택합니다.
21. vNIC 템플릿 목록에서 '사이트-01-iSCSI-A'를 선택합니다.
22. 어댑터 정책 드롭다운 목록에서 VMware 를 선택합니다.
23. 확인 을 클릭하여 이 vNIC를 정책에 추가합니다.

24. vNIC를 추가하려면 상단 추가 옵션을 클릭합니다.
25. vNIC 생성 대화 상자에서 vNIC 이름으로 Site-01-iscsi-B를 입력합니다.
26. vNIC 템플릿 사용 옵션을 선택합니다.
27. vNIC 템플릿 목록에서 '사이트-01-iSCSI-B'를 선택합니다.
28. 어댑터 정책 드롭다운 목록에서 VMware 를 선택합니다.
29. 확인 을 클릭하여 이 vNIC를 정책에 추가합니다.
30. iSCSI vNIC 추가 옵션을 확장합니다.
31. iSCSI vNIC 공간 추가 에서 아래쪽 추가 옵션을 클릭하여 iSCSI vNIC를 추가합니다.
32. iSCSI vNIC 생성 대화 상자에서 vNIC 이름으로 Site-01-iscsi-A를 입력합니다.
33. 오버레이 vNIC를 'ite-01-iscsi-a'로 선택합니다.
34. iSCSI 어댑터 정책 옵션을 Not Set로 둡니다.
35. VLAN을 Site-01-ISCSI-Site-A(NATIVE)로 선택합니다.
36. MAC 주소 할당으로 없음(기본값: 사용)을 선택합니다.
37. 확인 을 클릭하여 iSCSI vNIC를 정책에 추가합니다.



38. iSCSI vNIC 공간 추가 에서 아래쪽 추가 옵션을 클릭하여 iSCSI vNIC를 추가합니다.
39. iSCSI vNIC 생성 대화 상자에서 vNIC 이름으로 Site-01-iscsi-B를 입력합니다.
40. 오버레이 vNIC를 Site-01-iSCSI-B로 선택합니다
41. iSCSI 어댑터 정책 옵션을 Not Set로 둡니다.
42. VLAN을 Site-01-iSCSI-Site-B(NATIVE)로 선택합니다.
43. MAC 주소 할당으로 없음(기본값: 사용)을 선택합니다.
44. 확인 을 클릭하여 iSCSI vNIC를 정책에 추가합니다.
45. 변경 내용 저장 을 클릭합니다.



VMware ESXi 6.7U1 설치 부팅에 대한 **vMedia** 정책을 생성합니다

NetApp Data ONTAP 설정 단계에서는 NetApp Data ONTAP 및 VMware 소프트웨어를 호스팅하는 데 사용되는 HTTP 웹 서버가 필요합니다. 여기서 생성된 vMedia 정책은 VMware ESXi 6을 매핑합니다. 7U1 ISO를 클릭하여 ESXi 설치를 부팅합니다. 이 정책을 만들려면 다음 단계를 수행하십시오.

1. Cisco UCS Manager의 경우 왼쪽에서 서버 를 선택합니다.
2. 정책 > 루트를 선택합니다.
3. vMedia 정책 을 선택합니다.
4. 추가 를 클릭하여 새 vMedia 정책을 생성합니다.
5. 정책 이름을 ESXi-6.7U1-HTTP 로 지정합니다.
6. 설명 필드에 ESXi 6.7U1의 마운트 ISO를 입력합니다.
7. 마운트 실패 시 재시도를 위해 예를 선택하십시오.
8. 추가 를 클릭합니다.
9. 마운트 ESXi-6.7U1-HTTP의 이름을 지정합니다.
10. CDD Device Type을 선택한다.
11. HTTP 프로토콜을 선택합니다.
12. 웹 서버의 IP 주소를 입력합니다.

> DNS 서버 IP가 이전에 KVM IP에 입력되지 않았으므로 호스트 이름 대신 웹 서버의 IP를 입력해야 합니다.

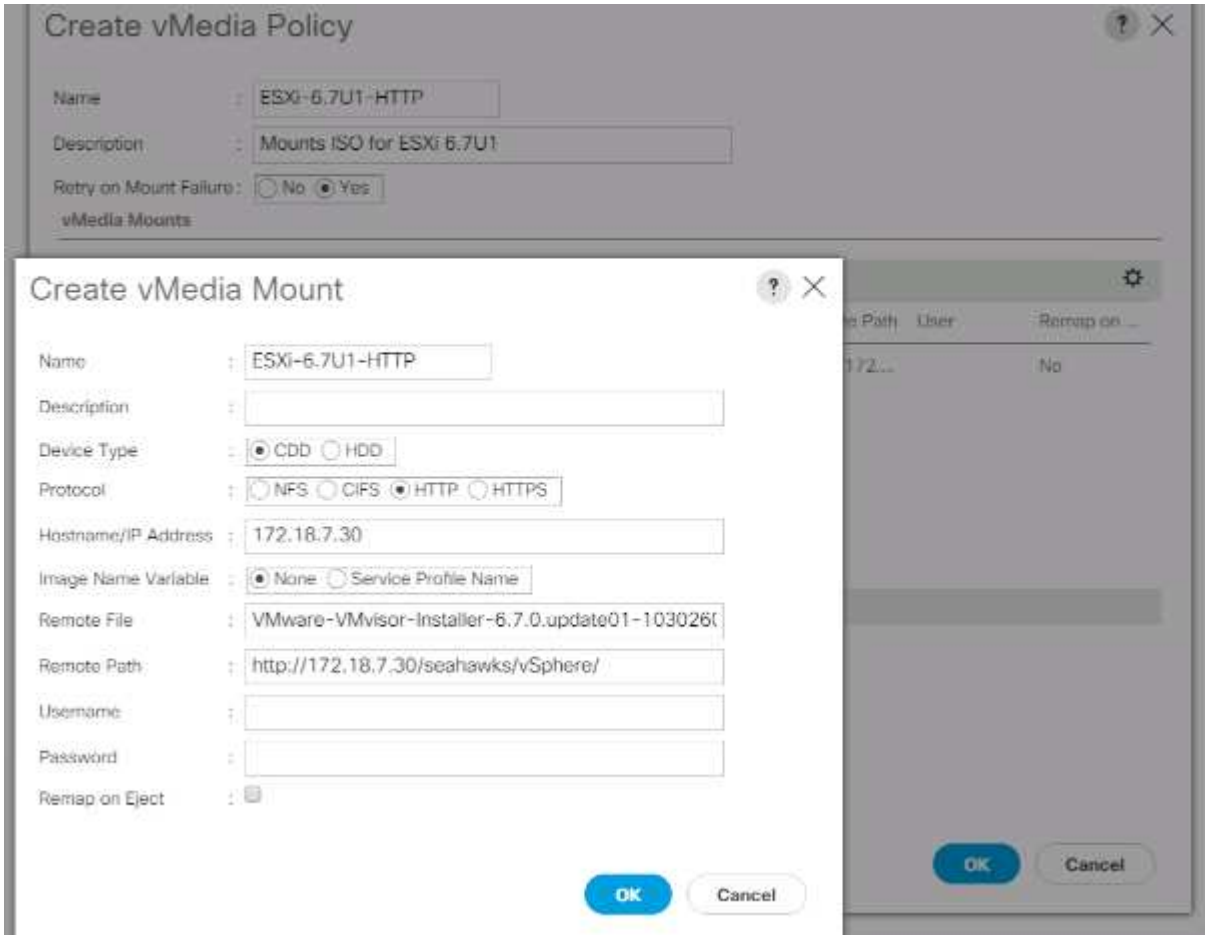
13. 원격 파일 이름으로 VMware-VMvisor-Installer-6.7.0.update01-10302608.x86_64.iso를 입력합니다.

    이 VMware ESXi 6.7U1 ISO는 에서 다운로드할 수 있습니다 "VMware 다운로드".

14. 원격 경로 필드에 ISO 파일의 웹 서버 경로를 입력합니다.

15. OK를 클릭하여 vMedia Mount를 생성합니다.
16. 확인 을 클릭한 다음 확인 을 다시 클릭하여 vMedia 정책 생성을 완료합니다.

Cisco UCS 환경에 추가된 새 서버의 경우 vMedia 서비스 프로필 템플릿을 사용하여 ESXi 호스트를 설치할 수 있습니다. SAN 마운트 디스크가 비어 있기 때문에 첫 번째 부팅 시 호스트가 ESXi 설치 프로그램으로 부팅됩니다. ESXi가 설치된 후에는 부팅 디스크에 액세스할 수 있는 한 vMedia가 참조되지 않습니다.



iSCSI 부트 정책을 생성합니다

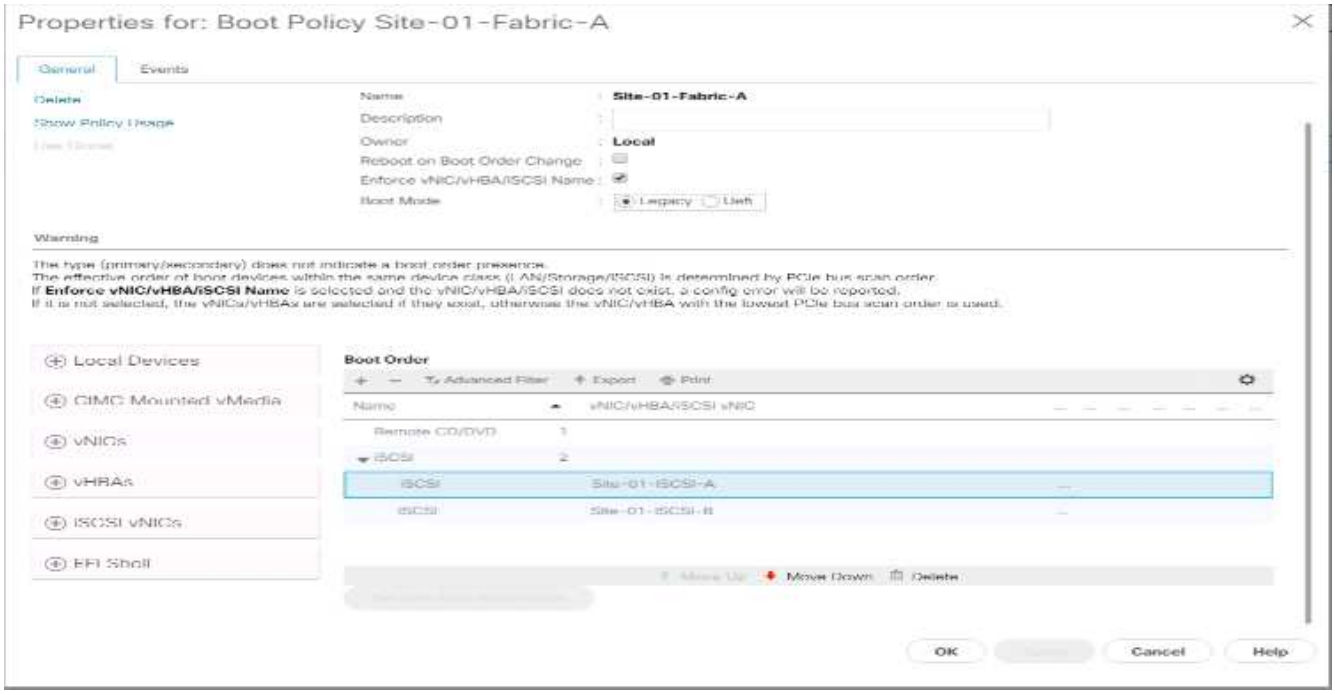
이 섹션의 절차는 두 개의 iSCSI 논리 인터페이스(LIF)가 클러스터 노드 1('iSCSI_liff 01a' 및 'iSCSI_liff')에 있고 두 개의 iSCSI LIF가 클러스터 노드 2('iscsi_liff 02a' 및 'iscsi_liff')에 있는 Cisco UCS 환경에 적용됩니다. 또한, LIF가 패브릭 A(Cisco UCS Fabric Interconnect A)에 연결되고 B LIF는 패브릭 B(Cisco UCS Fabric Interconnect B)에 연결되어 있다고 가정합니다.

ⓘ 이 절차에서 하나의 부팅 정책이 구성됩니다. 이 정책은 기본 대상을 "iscsi_liff 01a"로 구성합니다.

Cisco UCS 환경에 대한 부팅 정책을 생성하려면 다음 단계를 수행하십시오.

1. Cisco UCS Manager의 경우 왼쪽에 있는 서버 를 클릭합니다.
2. 정책 > 루트를 선택합니다.
3. Boot Policies 를 마우스 오른쪽 버튼으로 클릭합니다.
4. Create Boot Policy를 선택합니다.

5. 부팅 정책의 이름으로 '사이트-01-Fabric-A'를 입력합니다.
6. 선택 사항: 부팅 정책에 대한 설명을 입력합니다.
7. Boot Order Change(부팅 순서 변경) 옵션의 Reboot(재부팅) 옵션을 선택하지 않은 상태로 유지합니다.
8. 부팅 모드가 레거시입니다.
9. 로컬 장치 드롭다운 메뉴를 확장하고 원격 CD/DVD 추가 를 선택합니다.
10. iSCSI vNIC 드롭다운 메뉴를 확장하고 iSCSI 부팅 추가 를 선택합니다.
11. Add iSCSI Boot 대화 상자에서 'ite-01-iscsi-a'를 입력합니다. 확인 을 클릭합니다.
12. Add iSCSI Boot 를 선택합니다.
13. Add iSCSI Boot 대화 상자에서 'ite-01-iscsi-B'를 입력합니다. 확인 을 클릭합니다.
14. 확인 을 클릭하여 정책을 생성합니다.



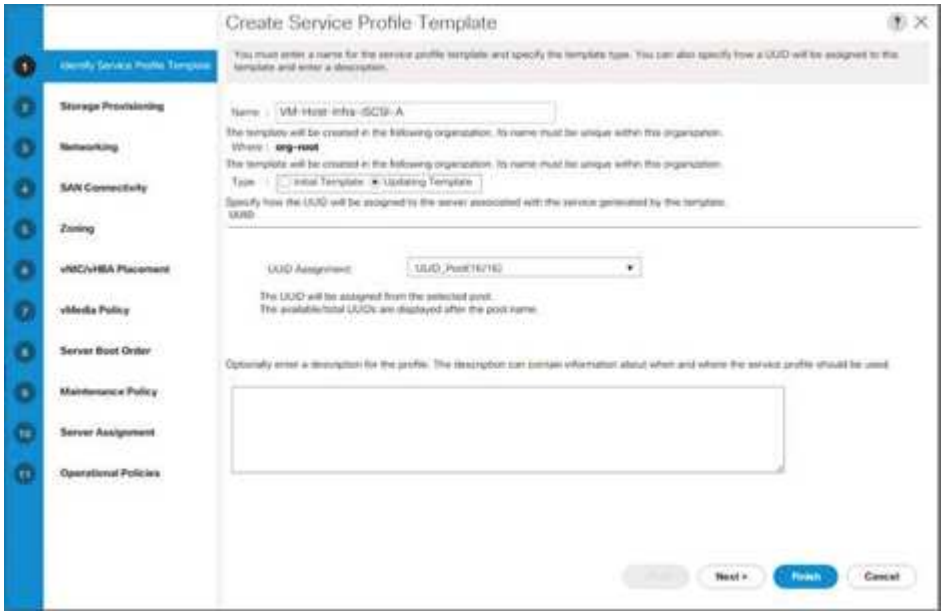
서비스 프로필 템플릿을 생성합니다

이 절차에서는 Fabric A 부팅을 위해 인프라스트럭처 ESXi 호스트에 대한 서비스 프로필 템플릿 하나가 생성됩니다.

서비스 프로필 템플릿을 생성하려면 다음 단계를 수행하십시오.

1. Cisco UCS Manager의 경우 왼쪽에 있는 서버 를 클릭합니다.
2. 서비스 프로필 템플릿 > 루트 를 선택합니다.
3. root 를 마우스 오른쪽 단추로 클릭합니다.
4. 서비스 프로필 템플릿 생성 을 선택하여 서비스 프로필 템플릿 생성 마법사를 엽니다.
5. 서비스 프로필 템플릿의 이름으로 VM-Host-Infra-iSCSI-A를 입력합니다. 이 서비스 프로필 템플릿은 패브릭 A의 스토리지 노드 1에서 부팅하도록 구성됩니다
6. 템플릿 업데이트 옵션을 선택합니다.

7. UUID에서 UUID 풀로 UUID_Pool을 선택합니다. 다음 을 클릭합니다.



스토리지 프로비저닝을 구성합니다

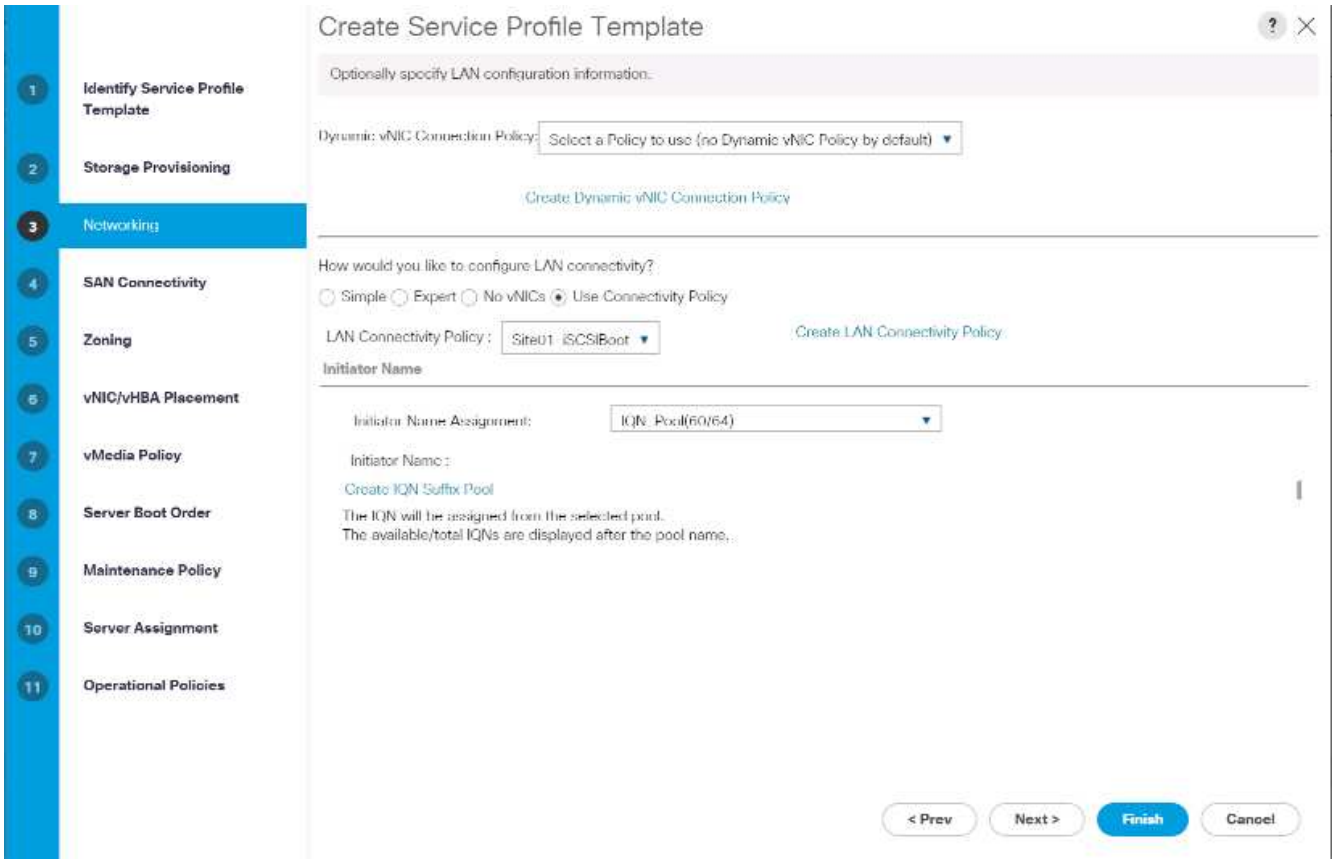
스토리지 프로비저닝을 구성하려면 다음 단계를 수행하십시오.

1. 물리적 디스크가 없는 서버가 있는 경우 로컬 디스크 구성 정책 을 클릭하고 SAN 부팅 로컬 스토리지 정책 을 선택합니다. 그렇지 않으면 기본 로컬 스토리지 정책을 선택합니다.
2. 다음 을 클릭합니다.

네트워킹 옵션을 구성합니다

네트워킹 옵션을 구성하려면 다음 단계를 수행하십시오.

1. 동적 vNIC 연결 정책의 기본 설정을 유지합니다.
2. 연결 정책 사용 옵션을 선택하여 LAN 연결을 구성합니다.
3. LAN 연결 정책 드롭다운 메뉴에서 iSCSI - 부팅 을 선택합니다.
4. 이니시에이터 이름 할당에서 IQN_Pool을 선택합니다. 다음 을 클릭합니다.



SAN 연결을 구성합니다

SAN 연결을 구성하려면 다음 단계를 수행하십시오.

1. vHBA의 경우 SAN 연결을 어떻게 구성하시겠습니까? 에서 아니요 를 선택합니다. 옵션을 선택합니다.
2. 다음 을 클릭합니다.

조닝을 구성합니다

조닝을 구성하려면 다음을 클릭합니다.

vNIC/HBA 배치를 구성합니다

vNIC/HBA 배치를 구성하려면 다음 단계를 수행하십시오.

1. Select Placement(배치 선택) 드롭다운 목록에서 배치 정책을 Let System Perform Placement(배치 수행) 로 둡니다.
2. 다음 을 클릭합니다.

vMedia 정책을 구성합니다

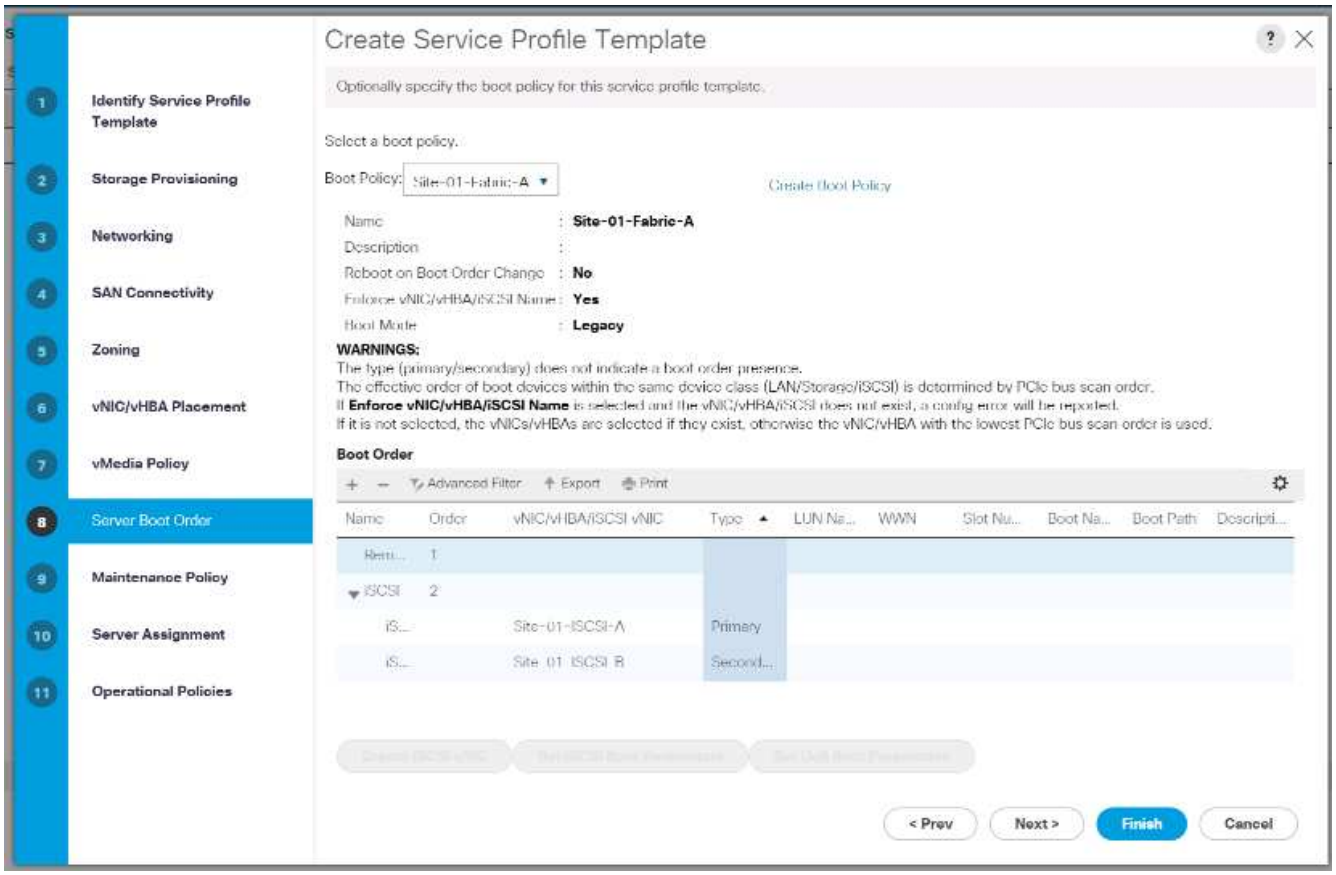
vMedia 정책을 구성하려면 다음 단계를 수행하십시오.

1. vMedia 정책을 선택하지 마십시오.
2. 다음 을 클릭합니다.

서버 부팅 순서를 구성합니다

서버 부팅 순서를 구성하려면 다음 단계를 수행하십시오.

1. Boot Policy에서 Boot-Fabric-A를 선택합니다.



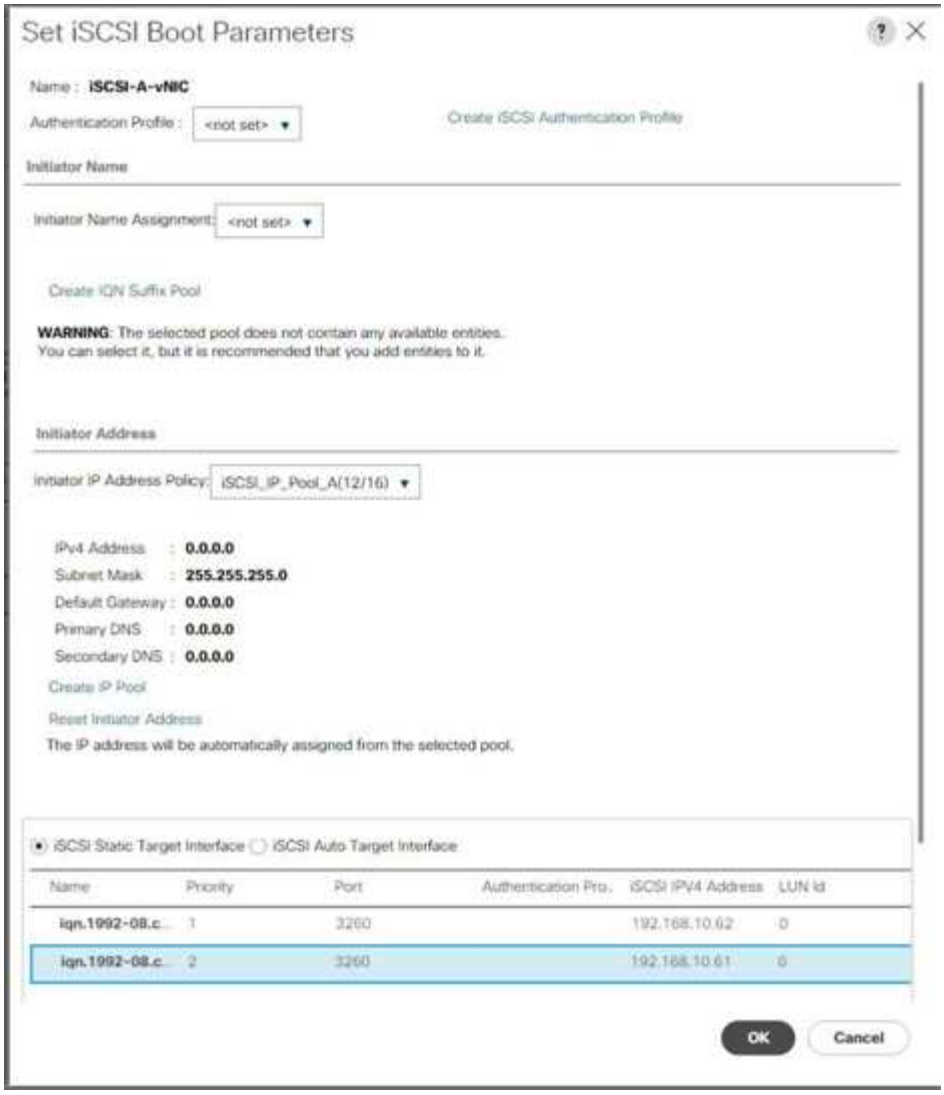
2. 보or 순서에서 '사이트-01-iSCSI-A'를 선택합니다.
3. Set iSCSI Boot Parameters(iSCSI 부팅 매개변수 설정) 를 클릭합니다.
4. iSCSI 부트 매개 변수 설정 대화 상자에서 환경에 적합한 인증 프로파일을 별도로 만들지 않은 경우 인증 프로파일 옵션을 설정하지 않음 으로 둡니다.
5. 이전 단계에서 정의한 단일 서비스 프로필 이니시에이터 이름을 사용하려면 이니시에이터 이름 할당 대화 상자를 Not Set로 두십시오.
6. "iscsi_ip_Pool_a"를 초기자 IP 주소 정책으로 설정합니다.
7. iSCSI 정적 타겟 인터페이스 옵션을 선택합니다.
8. 추가 를 클릭합니다.
9. iSCSI 타겟 이름을 입력합니다. Infra-SVM의 iSCSI 대상 이름을 얻으려면 스토리지 클러스터 관리 인터페이스에 로그인하고 "iscsi show" 명령을 실행합니다.

```
bb04-aff300::> iscsi show
          Target                          Target                          Status
Vserver   Name                            Alias                           Admin
--------- ------------------------------- ------------------------------- ------
Infra-SVM iqn.1992-08.com.netapp:sn.b5acab9ef1c811e68d9d00a098a9fec2:vs.3
                                          Infra-SVM                       up
```

10. IPv4 Address 필드에 iSCSI_lif_02a IP 주소를 입력합니다.

11. 확인 을 클릭하여 iSCSI 정적 대상을 추가합니다.
12. 추가 를 클릭합니다.
13. iSCSI 타겟 이름을 입력합니다.
14. IPv4 Address 필드에 iSCSI_lif_01A IP 주소를 입력합니다.

15. 확인 을 클릭하여 iSCSI 정적 대상을 추가합니다.



타겟 IP는 스토리지 노드 02 IP를 먼저, 스토리지 노드 01 IP와 함께 배치되었습니다. 부팅 LUN이 노드 01에 있다고 가정합니다. 이 절차의 순서가 사용되는 경우 호스트는 노드 01의 경로를 사용하여 부팅됩니다.

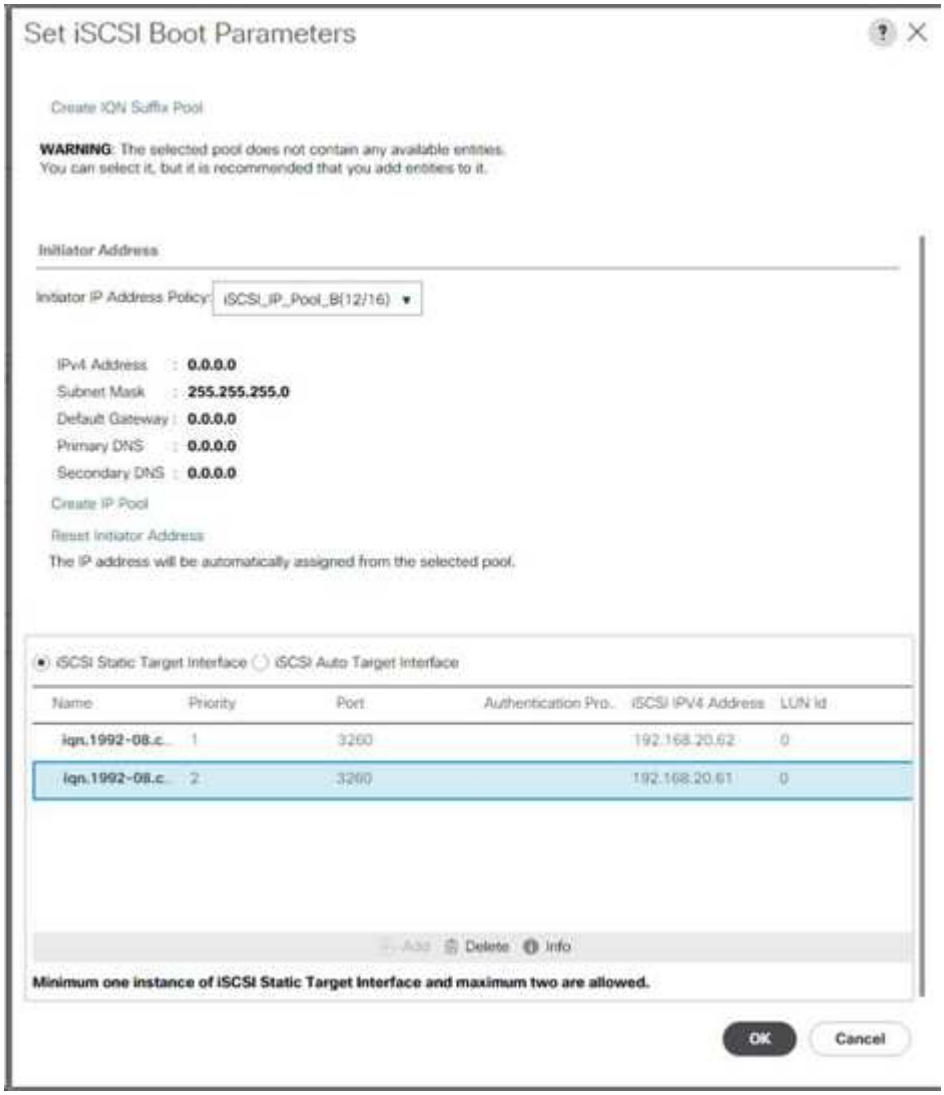
16. 부팅 순서에서 iSCSI-B-vNIC를 선택합니다.
17. Set iSCSI Boot Parameters(iSCSI 부팅 매개변수 설정) 를 클릭합니다.
18. iSCSI 부트 매개 변수 설정 대화 상자에서 환경에 적합한 인증 프로파일을 별도로 만들지 않은 경우 인증 프로파일 옵션을 설정되지 않음 으로 둡니다.
19. 이전 단계에서 정의한 단일 서비스 프로필 이니시에이터 이름을 사용하려면 이니시에이터 이름 할당 대화 상자를 Not Set로 두십시오.
20. ISCSI_IP_Pool_B를 초기자 IP 주소 정책으로 설정합니다.
21. iSCSI 정적 타겟 인터페이스 옵션을 선택합니다.
22. 추가 를 클릭합니다.
23. iSCSI 타겟 이름을 입력합니다. Infra-SVM의 iSCSI 대상 이름을 얻으려면 스토리지 클러스터 관리 인터페이스에 로그인하고 "iscsi show" 명령을 실행합니다.

```
bb04-aff300::> iscsi show
          Target                          Target                          Status
Vserver   Name                            Alias                           Admin
--------- ------------------------------- ------------------------------- ------
Infra-SVM  iqn.1992-08.com.netapp:sn.b5acab9ef1c811e68d9d00a098a9fec2:vs.3
                                          Infra-SVM                       up
```

24. IPv4 Address 필드에 iSCSI_lif_02B의 IP 주소를 입력합니다.

25. 확인 을 클릭하여 iSCSI 정적 대상을 추가합니다.
26. 추가 를 클릭합니다.
27. iSCSI 타겟 이름을 입력합니다.
28. IPv4 Address 필드에 iSCSI_lif_01B IP 주소를 입력합니다.

29. 확인 을 클릭하여 iSCSI 정적 대상을 추가합니다.

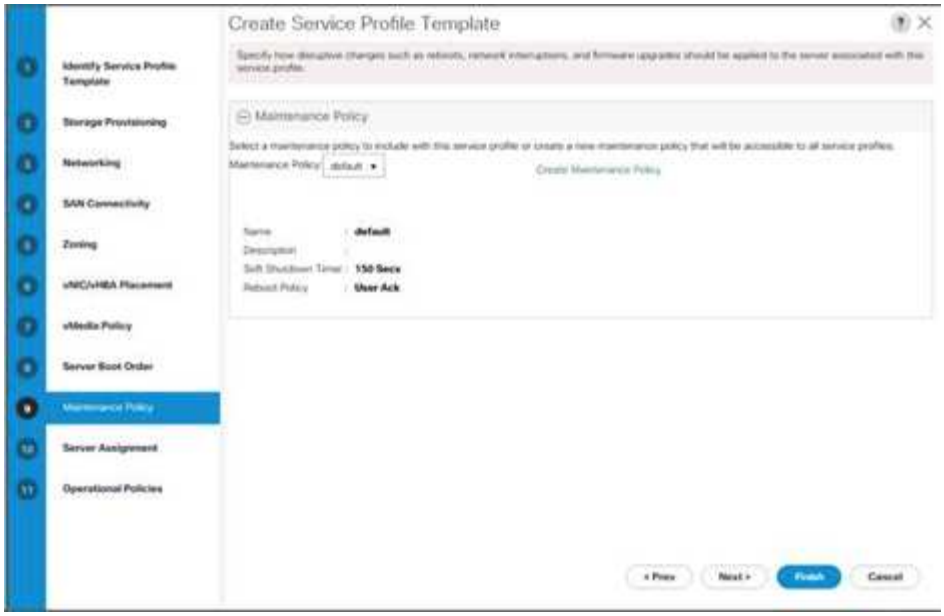


30. 다음 을 클릭합니다.

유지 관리 정책을 구성합니다

유지보수 정책을 구성하려면 다음 단계를 완료하십시오.

1. 유지보수 정책을 기본값으로 변경합니다.

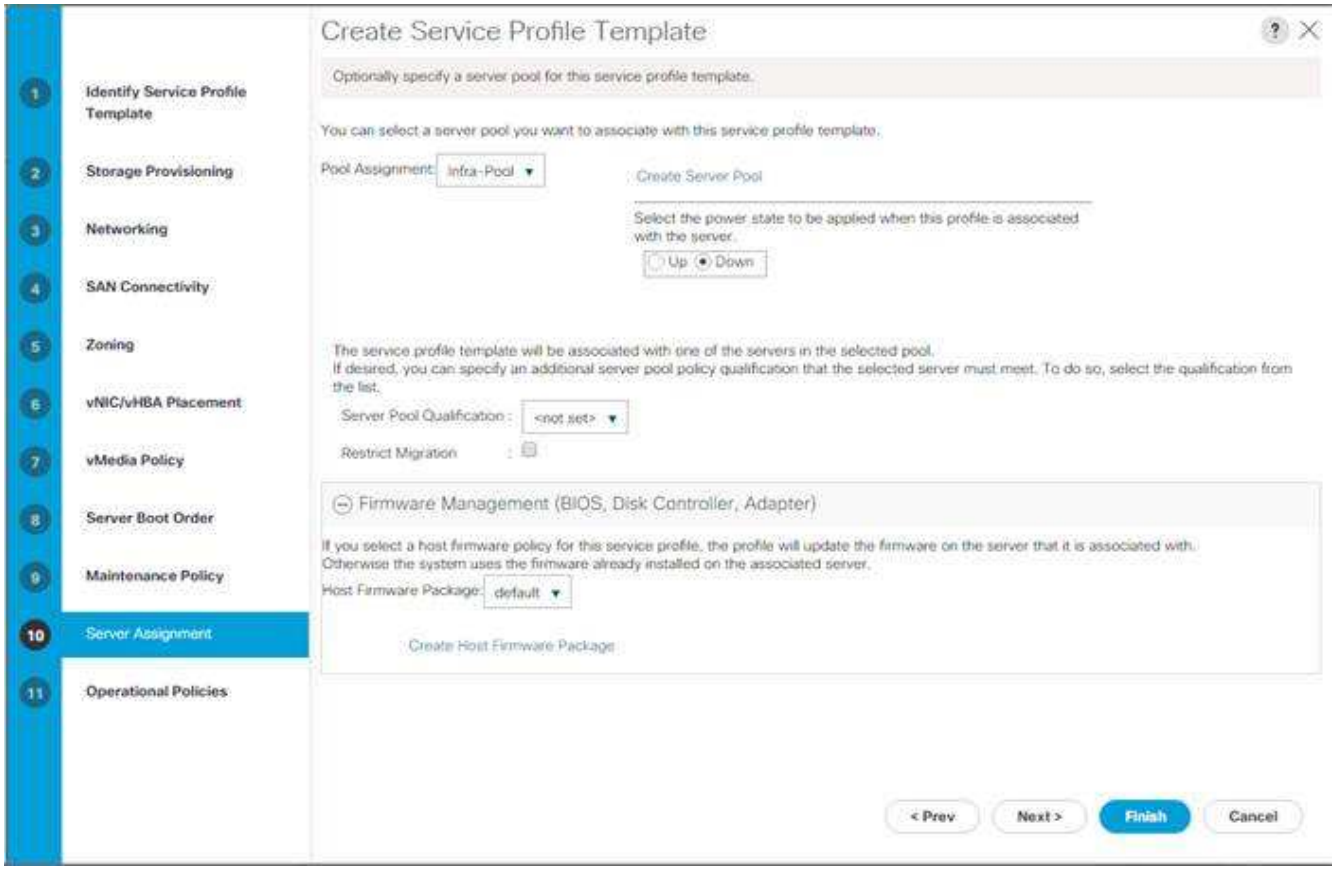


2. 다음 을 클릭합니다.

서버 할당을 구성합니다

서버 할당을 구성하려면 다음 단계를 완료하십시오.

1. 풀 할당 목록에서 Infra-Pool을 선택합니다.
2. 프로파일이 서버에 연결될 때 적용될 전원 상태로 down(끄기)을 선택합니다.
3. 페이지 하단의 펌웨어 관리 를 확장하고 기본 정책을 선택합니다.

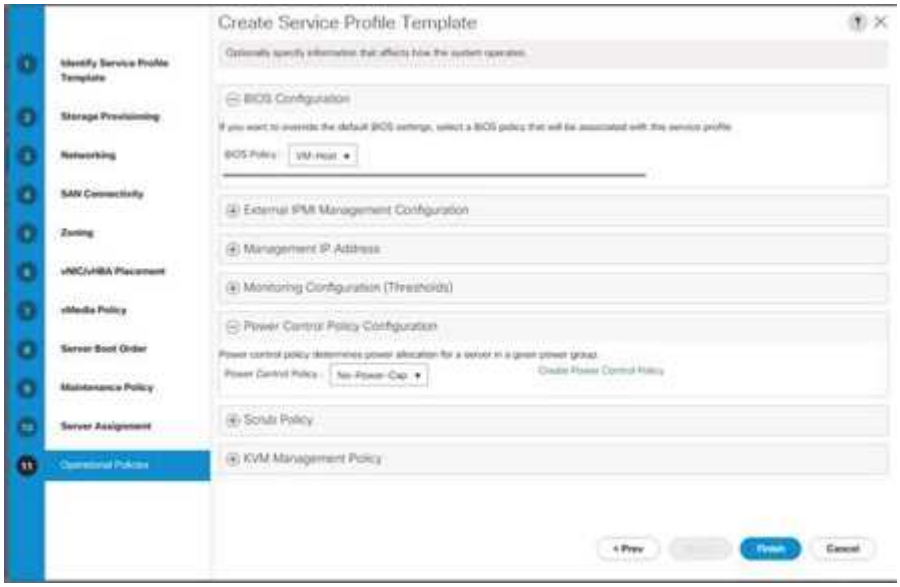


4. 다음 을 클릭합니다.

운영 정책을 구성합니다

운영 정책을 구성하려면 다음 단계를 완료하십시오.

1. BIOS 정책 드롭다운 목록에서 VM-호스트 를 선택합니다.
2. 전원 제어 정책 구성 을 확장하고 전원 제어 정책 드롭다운 목록에서 전원이 들어오지 않음(No Power-Cap) 을 선택합니다.



3. 마침 을 클릭하여 서비스 프로필 템플릿을 생성합니다.
4. 확인 메시지에서 확인 을 클릭합니다.

vMedia 지원 서비스 프로필 템플릿을 생성합니다

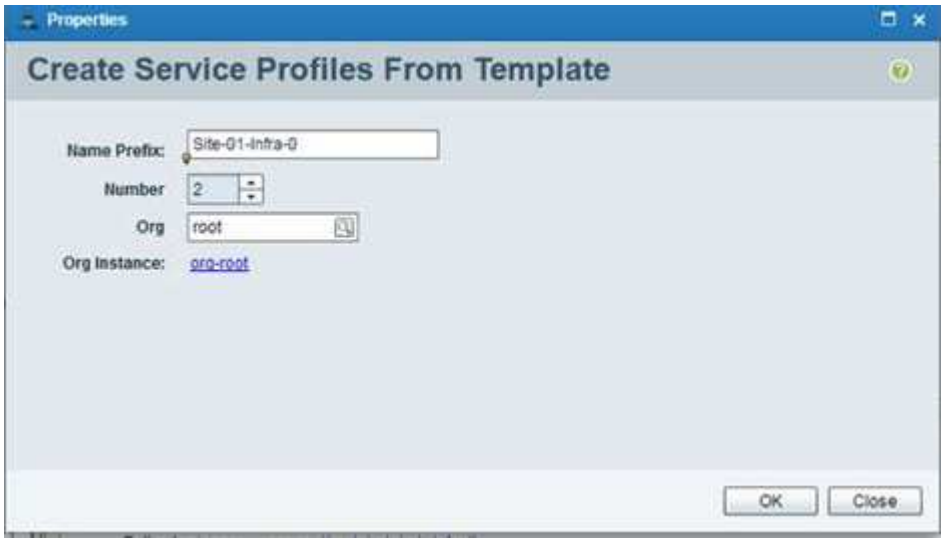
vMedia가 활성화된 서비스 프로필 템플릿을 생성하려면 다음 단계를 수행하십시오.

1. UCS Manager에 연결하고 왼쪽에서 서버 를 클릭합니다.
2. 서비스 프로필 템플릿 > 루트 > 서비스 템플릿 VM-호스트-인프라스트럭처-iSCSI-A를 선택합니다
3. VM-Host-Infra-iSCSI-A를 마우스 오른쪽 버튼으로 클릭하고 Create a Clone을 선택합니다.
4. 클론 이름을 VM-Host-Infra-iSCSI-A-VM으로 지정합니다.
5. 새로 생성된 VM-Host-Infra-iSCSI-A-VM을 선택하고 오른쪽에서 vMedia Policy 탭을 선택합니다.
6. vMedia 정책 수정을 클릭합니다.
7. ESXi-6을 선택합니다. 7U1-HTTP vMedia 정책 을 클릭하고 확인 을 클릭합니다.
8. 확인을 클릭하여 확인합니다.

서비스 프로필을 생성합니다

서비스 프로필 템플릿에서 서비스 프로필을 생성하려면 다음 단계를 수행하십시오.

1. Cisco UCS Manager에 연결하고 왼쪽에서 서버 를 클릭합니다.
2. Servers > Service Profile Templates > root > Service Template <name> 을 확장합니다.
3. 동작에서 템플릿으로부터 서비스 프로필 만들기를 클릭하고 다음 단계를 경쟁합니다.
   a. 이름 접두사로 'ite-01-infra-0'을 입력합니다.
   b. 생성할 인스턴스 수로 2를 입력합니다.
   c. ORG로 root를 선택합니다.
   d. 확인 을 클릭하여 서비스 프로필을 만듭니다.



4. 확인 메시지에서 확인 을 클릭합니다.

5. 서비스프로필 ite-01-Infra-01과 Site-01-Infra-02가 만들어졌는지 확인한다.

   서비스 프로필은 할당된 서버 풀의 서버와 자동으로 연결됩니다.

스토리지 구성 2부: 부팅 LUN 및 이니시에이터 그룹

ONTAP 부팅 저장소 설정

이니시에이터 그룹을 생성합니다

이니시에이터 그룹(igroup)을 생성하려면 다음 단계를 완료합니다.

1. 클러스터 관리 노드의 SSH 연결에서 다음 명령을 실행합니다.

```
igroup create –vserver Infra-SVM –igroup VM-Host-Infra-01 –protocol
iscsi –ostype vmware –initiator <vm-host-infra-01-iqn>
igroup create –vserver Infra-SVM –igroup VM-Host-Infra-02 –protocol
iscsi –ostype vmware –initiator <vm-host-infra-02-iqn>
igroup create –vserver Infra-SVM –igroup MGMT-Hosts –protocol iscsi
–ostype vmware –initiator <vm-host-infra-01-iqn>, <vm-host-infra-02-iqn>
```

   IQN 정보에 대해서는 표 1 및 표 2에 나열된 값을 사용합니다.

2. 방금 작성한 3개 igroup을 보려면 'igroup show' 명령을 실행합니다.

부팅 LUN을 igroup에 매핑합니다

부팅 LUN을 igroup에 매핑하려면 다음 단계를 완료하십시오.

1. 스토리지 클러스터 관리 SSH 연결에서 다음 명령을 실행합니다.

```
lun map –vserver Infra-SVM –volume esxi_boot –lun VM-Host-Infra- A
–igroup VM-Host-Infra-01 –lun-id 0lun map –vserver Infra-SVM –volume
esxi_boot –lun VM-Host-Infra- B –igroup VM-Host-Infra-02 –lun-id 0
```

VMware vSphere 6.7U1 구축 절차

이 섹션에서는 FlexPod Express 구성에 VMware ESXi 6.7U1을 설치하는 절차를 자세히 설명합니다. 절차가 완료된 후 부팅된 ESXi 호스트 2개가 프로비저닝됩니다.

VMware 환경에 ESXi를 설치하는 방법은 여러 가지가 있습니다. 이 절차에서는 Cisco UCS Manager에 내장된 KVM 콘솔과 가상 미디어 기능을 사용하여 원격 설치 미디어를 개별 서버에 매핑하고 부팅 LUN에 연결하는 방법에 초점을 맞춥니다.

ESXi 6.7U1용 Cisco 사용자 지정 이미지를 다운로드합니다

VMware ESXi 사용자 지정 이미지를 다운로드하지 않은 경우 다음 단계를 수행하여 다운로드를 완료합니다.

1. https://my.vmware.com/group/vmware/details?downloadGroup=OEM-ESXI67U1-CISCO&productId=742[VMware vSphere 하이퍼바이저(ESXi) 6.7U1.^ 링크를 클릭합니다.
2. 에 사용자 ID와 암호가 필요합니다 "VMware.com" 를 눌러 이 소프트웨어를 다운로드합니다.
3. ISO 파일을 다운로드합니다.

Cisco UCS Manager를 참조하십시오

Cisco UCS IP KVM을 사용하면 관리자가 원격 미디어를 통해 OS 설치를 시작할 수 있습니다. IP KVM을 실행하려면 Cisco UCS 환경에 로그인해야 합니다.

Cisco UCS 환경에 로그인하려면 다음 단계를 수행하십시오.

1. 웹 브라우저를 열고 Cisco UCS 클러스터 주소의 IP 주소를 입력합니다. 이 단계에서는 Cisco UCS Manager 애플리케이션을 시작합니다.
2. HTML에서 UCS Manager 실행 링크를 클릭하여 HTML 5 UCS Manager GUI를 시작합니다.
3. 보안 인증서를 수락하라는 메시지가 나타나면 필요에 따라 수락하십시오.
4. 메시지가 나타나면 사용자 이름으로 admin을 입력하고 관리자 암호를 입력합니다.
5. Cisco UCS Manager에 로그인하려면 로그인을 클릭합니다.
6. 기본 메뉴에서 왼쪽에 있는 서버 를 클릭합니다.
7. Servers > Service Profiles > root > VM-Host-Infra-01’을 선택합니다.
8. VM-Host-Infra-01을 마우스 오른쪽 버튼으로 클릭하고 KVM Console을 선택합니다.
9. 표시되는 메시지에 따라 Java 기반 KVM 콘솔을 실행합니다.
10. Servers > Service Profiles > root > VM-Host-Infra-02’를 선택합니다.
11. VM-Host-Infra-02를 마우스 오른쪽 버튼으로 클릭합니다. KVM 콘솔을 선택합니다.
12. 표시되는 메시지에 따라 Java 기반 KVM 콘솔을 실행합니다.

VMware ESXi 설치를 설정합니다

ESXi 호스트 VM-Host-Infra-01 및 VM-Host-Infra-02

OS 설치를 위해 서버를 준비하려면 각 ESXi 호스트에서 다음 단계를 수행하십시오.

1. KVM 창에서 가상 미디어를 클릭합니다.
2. 가상 장치 활성화 를 클릭합니다.
3. 암호화되지 않은 KVM 세션을 수락하라는 메시지가 표시되면 필요에 따라 수락하십시오.
4. 가상 미디어 를 클릭하고 CD/DVD 매핑 을 선택합니다.
5. ESXi 설치 관리자 ISO 이미지 파일을 찾아 이동하고 Open을 클릭합니다.
6. 장치 매핑 을 클릭합니다.
7. KVM 탭을 클릭하여 서버 부팅을 모니터링합니다.

◦ ESXi * 설치

ESXi 호스트 VM-Host-Infra-01 및 VM-Host-Infra-02

호스트의 iSCSI 부팅 가능 LUN에 VMware ESXi를 설치하려면 각 호스트에서 다음 단계를 수행하십시오.

1. Boot Server를 선택하고 OK를 클릭하여 서버를 부팅합니다. 그런 다음 확인을 다시 클릭합니다.
2. 재부팅 시 ESXi 설치 미디어의 존재 여부가 자동으로 감지됩니다. 표시되는 부팅 메뉴에서 ESXi 설치 프로그램을 선택합니다.
3. 설치 프로그램 로드가 완료된 후 Enter 키를 눌러 설치를 계속합니다.
4. 최종 사용자 사용권 계약(EULA)을 읽고 동의합니다. F11 키를 눌러 동의하고 계속합니다.
5. 이전에 ESXi용 설치 디스크로 설정된 LUN을 선택하고 Enter 키를 눌러 설치를 계속합니다.
6. 적절한 자판 배열을 선택하고 Enter 키를 누릅니다.
7. 루트 암호를 입력 및 확인하고 Enter 키를 누릅니다.
8. 설치 프로그램에서 선택한 디스크가 다시 분할된다는 경고를 표시합니다. F11 키를 눌러 설치를 계속합니다.
9. 설치가 완료되면 Virtual Media 탭을 선택하고 ESXi 설치 미디어 옆에 있는 P 표시를 지웁니다. 예 를 클릭합니다.

설치 프로그램이 아닌 ESXi로 서버를 재부팅하도록 ESXi 설치 이미지를 매핑 해제해야 합니다.

10. 설치가 완료되면 Enter 키를 눌러 서버를 재부팅합니다.
11. Cisco UCS Manager에서 현재 서비스 프로필을 비 vMedia 서비스 프로필 템플릿에 바인딩하여 HTTP를 통해 ESXi 설치 ISO가 마운트되지 않도록 합니다.

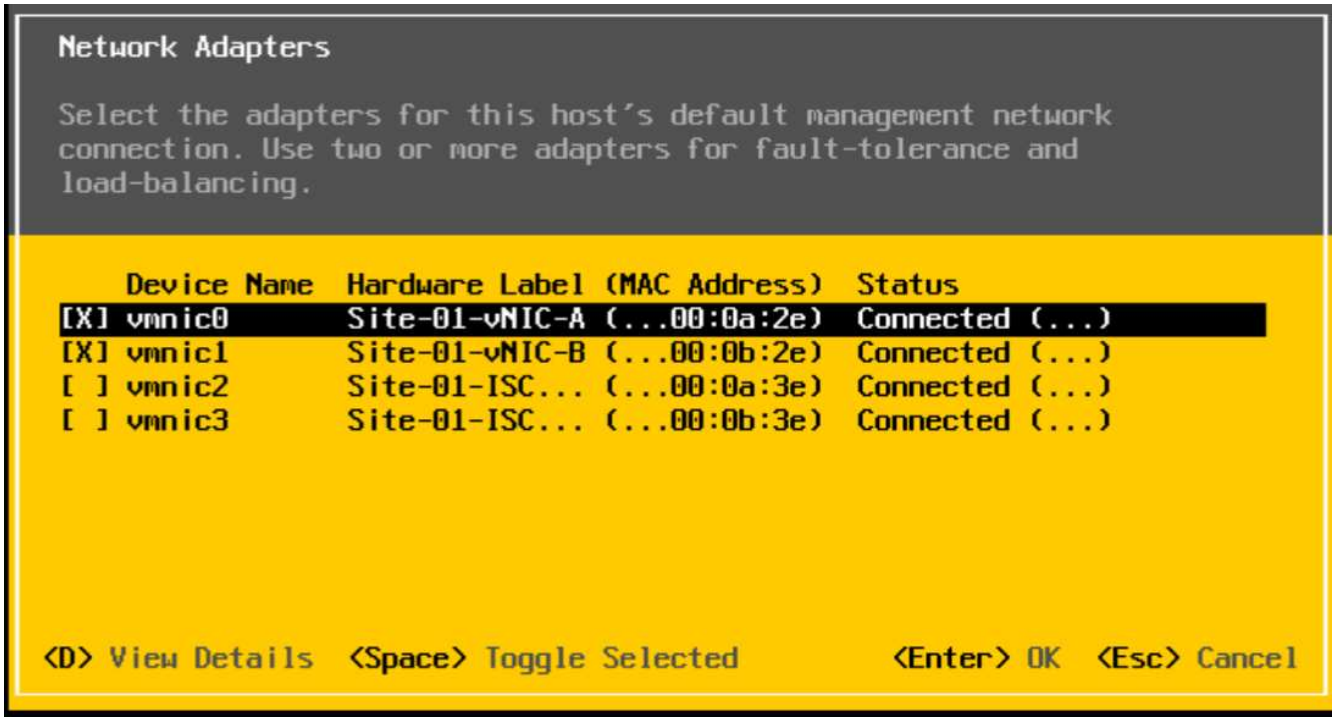
ESXi 호스트에 대한 관리 네트워킹을 설정합니다

호스트를 관리하려면 각 VMware 호스트에 대한 관리 네트워크를 추가해야 합니다. VMware 호스트에 대한 관리 네트워크를 추가하려면 각 ESXi 호스트에서 다음 단계를 수행합니다.

ESXi 호스트 VM-Host-Infra-01 및 VM-Host-Infra-02

관리 네트워크에 액세스할 수 있도록 각 ESXi 호스트를 구성하려면 다음 단계를 수행하십시오.

1. 서버 재부팅이 완료된 후 F2 키를 눌러 시스템을 사용자 정의합니다.
2. root로 로그인하여 해당 비밀번호를 입력한 후 Enter를 눌러 로그인합니다.
3. 문제 해결 옵션을 선택하고 Enter 키를 누릅니다.
4. ESXi 셸 활성화 를 선택하고 Enter 키를 누릅니다.
5. SSH 활성화 를 선택하고 Enter 키를 누릅니다.
6. Esc 키를 눌러 문제 해결 옵션 메뉴를 종료합니다.
7. Configure Management Network 옵션을 선택하고 Enter 키를 누릅니다.
8. Network Adapters 를 선택하고 Enter 키를 누릅니다.
9. 하드웨어 레이블 필드의 숫자가 장치 이름 필드의 번호와 일치하는지 확인합니다.
10. Enter 키를 누릅니다.



11. VLAN (Optional) 옵션을 선택하고 Enter 키를 누릅니다.
12. '<IB-mgmt-vlan-id>'를 입력하고 Enter 키를 누릅니다.
13. IPv4 구성 을 선택하고 Enter 키를 누릅니다.
14. 스페이스바를 사용하여 정적 IPv4 주소 설정 및 네트워크 구성 옵션을 선택합니다.
15. 첫 번째 ESXi 호스트를 관리하기 위한 IP 주소를 입력합니다.
16. 첫 번째 ESXi 호스트의 서브넷 마스크를 입력합니다.
17. 첫 번째 ESXi 호스트의 기본 게이트웨이를 입력합니다.
18. Enter 키를 눌러 IP 구성의 변경 사항을 적용합니다.
19. DNS 구성 옵션을 선택하고 Enter 키를 누릅니다.

    IP 주소는 수동으로 할당되므로 DNS 정보도 수동으로 입력해야 합니다.

20. 기본 DNS 서버의 IP 주소를 입력합니다.
21. 선택 사항: 보조 DNS 서버의 IP 주소를 입력합니다.
22. 첫 번째 ESXi 호스트의 FQDN을 입력합니다.
23. Enter 키를 눌러 DNS 구성의 변경 사항을 적용합니다.
24. Esc를 눌러 Configure Management Network 메뉴를 종료합니다.
25. 관리 네트워크 테스트 를 선택하여 관리 네트워크가 올바르게 설정되어 있는지 확인하고 Enter 키를 누릅니다.
26. Enter 키를 눌러 테스트를 실행하고 테스트가 완료되면 Enter 키를 다시 누릅니다. 오류가 발생하면 환경을 검토합니다.
27. Configure Management Network를 다시 선택하고 Enter 키를 누릅니다.
28. IPv6 구성 옵션을 선택하고 Enter 키를 누릅니다.

29. 스페이스바를 사용하여 Disable IPv6 (restart required) 를 선택하고 Enter 키를 누릅니다.
30. Esc 키를 눌러 Configure Management Network 하위 메뉴를 종료합니다.
31. Y 를 눌러 변경 사항을 확인하고 ESXi 호스트를 재부팅합니다.

VMware ESXi 호스트 **VMkernel** 포트 **vmk0 MAC** 주소 재설정**(**선택 사항**)**

ESXi 호스트 VM-Host-Infra-01 및 VM-Host-Infra-02

기본적으로 관리 VMkernel 포트 vmk0의 MAC 주소는 관리 VMkernel 포트가 배치된 이더넷 포트의 MAC 주소와 동일합니다. ESXi 호스트의 부팅 LUN이 다른 MAC 주소를 가진 다른 서버에 다시 매핑되면 ESXi 시스템 구성이 재설정되지 않는 한 vmk0이 할당된 MAC 주소를 유지하므로 MAC 주소 충돌이 발생합니다. vmk0의 MAC 주소를 임의의 VMware 할당 MAC 주소로 재설정하려면 다음 단계를 수행하십시오.

1. ESXi 콘솔 메뉴 기본 화면에서 Ctrl-Alt-F1을 눌러 VMware 콘솔 명령줄 인터페이스에 액세스합니다. UCSM KVM에서 Ctrl-Alt-F1이 정적 매크로 목록에 나타납니다.
2. 루트로 로그인합니다.
3. 인터페이스 vmk0의 세부 목록을 보려면 esxcfg-vmknic –l을 입력하십시오. vmk0은 Management Network 포트 그룹에 속해야 합니다. vmk0의 IP 주소와 넷마스크를 기록해 둡니다.
4. vmk0을 제거하려면 다음 명령을 입력합니다.

```
esxcfg-vmknic –d “Management Network”
```

5. 임의의 MAC 주소를 사용하여 vmk0을 다시 추가하려면 다음 명령을 입력합니다.

```
esxcfg-vmknic –a –i <vmk0-ip> -n <vmk0-netmask> “Management Network””.
```

6. 임의의 MAC 주소를 사용하여 vmk0이 다시 추가되었는지 확인합니다

```
esxcfg-vmknic –l
```

7. 명령줄 인터페이스에서 로그아웃하려면 "exit"를 입력합니다.
8. Ctrl-Alt-F2를 눌러 ESXi 콘솔 메뉴 인터페이스로 돌아갑니다.

VMware 호스트 클라이언트를 사용하여 **VMware ESXi** 호스트에 로그인합니다

ESXi 호스트 VM-Host-Infra-01

VMware 호스트 클라이언트를 사용하여 VM-Host-Infra-01 ESXi 호스트에 로그인하려면 다음 단계를 수행하십시오.

1. 관리 워크스테이션에서 웹 브라우저를 열고 VM-Host-Infra-01 관리 IP 주소로 이동합니다.
2. VMware 호스트 클라이언트 열기 를 클릭합니다.
3. 사용자 이름으로 root를 입력합니다.

4. 루트 암호를 입력합니다.
5. Login을 클릭하여 연결합니다.
6. 이 과정을 반복하여 별도의 브라우저 탭이나 창에서 VM-Host-Infra-02에 로그인합니다.

VIC(Cisco Virtual Interface Card)용 VMware 드라이버 설치

다음 VMware VIC 드라이버에 대한 오프라인 번들을 다운로드하여 관리 워크스테이션에 압축을 풉니다.

- nenic 드라이버 버전 1.0.25.0

ESXi는 VM-Host-Infra-01 및 VM-Host-Infra-02를 호스팅합니다

ESXi 호스트 VM-Host-Infra-01 및 VM-Host-Infra-02에 VMware VIC 드라이버를 설치하려면 다음 단계를 수행하십시오.

1. 각 호스트 클라이언트에서 스토리지를 선택합니다.
2. datastore1을 마우스 오른쪽 단추로 클릭하고 찾아보기 를 선택합니다.
3. 데이터 저장소 브라우저에서 업로드 를 클릭합니다.
4. 다운로드한 VIC 드라이버의 저장된 위치로 이동하고 VMW-ESX-6.7.0-nenic-1.0.25.0-offline_bundle-11271332.zip을 선택합니다.
5. 데이터 저장소 브라우저에서 업로드 를 클릭합니다.
6. 열기 를 클릭하여 파일을 datastore1에 업로드합니다.
7. 파일이 두 ESXi 호스트에 모두 업로드되었는지 확인합니다.
8. 각 호스트를 유지 관리 모드로 전환합니다(아직 없는 경우).
9. 셸 연결 또는 putty 터미널에서 ssh를 통해 각 ESXi 호스트에 연결합니다.
10. 루트 암호를 사용하여 루트로 로그인합니다.
11. 각 호스트에서 다음 명령을 실행합니다.

```
esxcli software vib update -d /vmfs/volumes/datastore1/VMW-ESX-6.7.0-
nenic-1.0.25.0-offline_bundle-11271332.zip
reboot
```

12. 재부팅이 완료되면 각 호스트의 호스트 클라이언트에 로그인하고 유지 관리 모드를 종료합니다.

VMkernel 포트 및 가상 스위치를 설정합니다

ESXi 호스트 VM-Host-Infra-01 및 VM-Host-Infra-02

ESXi 호스트에서 VMkernel 포트 및 가상 스위치를 설정하려면 다음 단계를 수행하십시오.

1. 호스트 클라이언트 의 왼쪽에서 네트워킹 을 선택합니다.
2. 가운데 창에서 가상 스위치 탭을 선택합니다.
3. vSwitch0을 선택합니다.

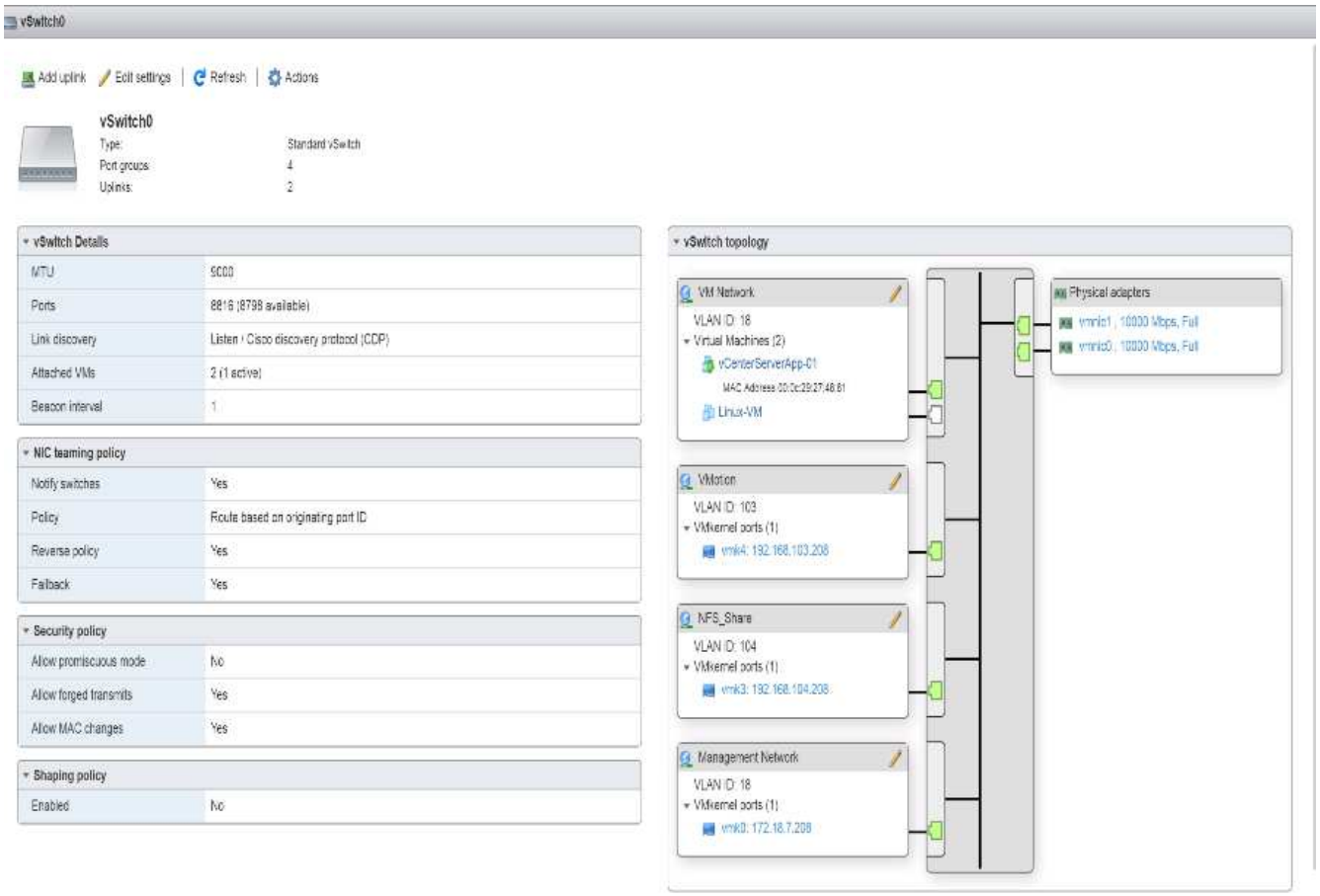
4. 설정 편집 을 선택합니다.
5. MTU를 9000으로 변경합니다.
6. NIC 팀 구성을 확장합니다.
7. 페일오버 순서 섹션에서 vmnic1을 선택하고 활성 상태로 표시를 클릭합니다.
8. vmnic1의 상태가 활성인지 확인합니다.
9. 저장 을 클릭합니다.
10. 왼쪽에서 네트워킹 을 선택합니다.
11. 가운데 창에서 가상 스위치 탭을 선택합니다.
12. iSciBootvSwitch 를 선택합니다.
13. 설정 편집 을 선택합니다.
14. MTU를 9000으로 변경합니다
15. 저장 을 클릭합니다.
16. VMkernel NIC 탭을 선택합니다.
17. vmk1 iSciBootPG 를 선택합니다.
18. 설정 편집 을 선택합니다.
19. MTU를 9000으로 변경합니다.
20. IPv4 설정을 확장하고 IP 주소를 UCS iSCSI-IP-Pool-A 외부의 주소로 변경합니다

> Cisco UCS iSCSI IP 풀 주소를 재할당해야 하는 경우 IP 주소 충돌을 방지하려면 iSCSI VMkernel 포트에 대해 동일한 서브넷에 있는 다른 IP 주소를 사용하는 것이 좋습니다.

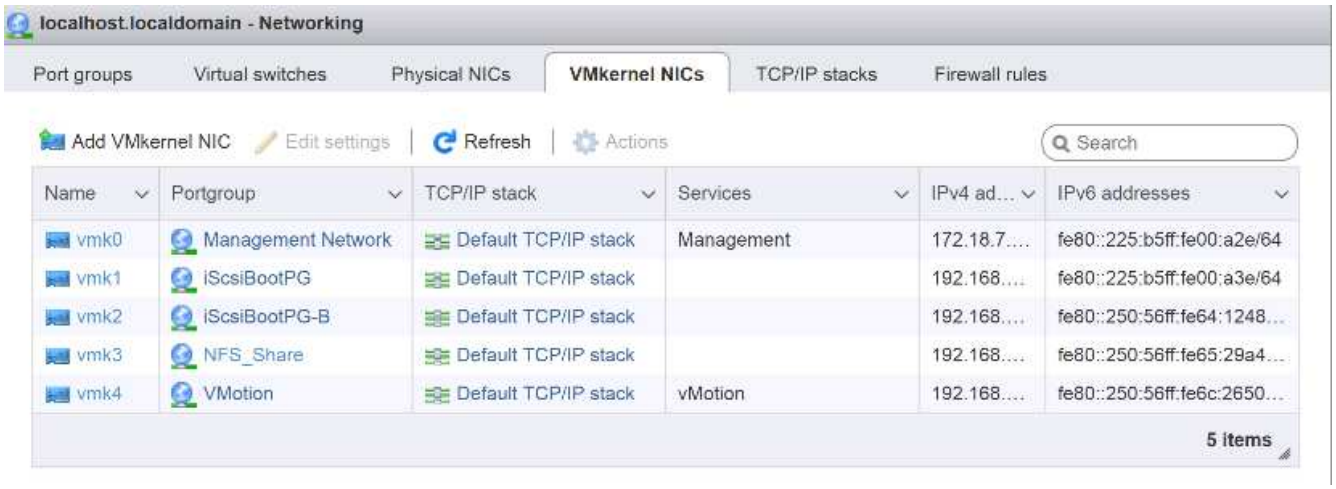
21. 저장 을 클릭합니다.
22. 가상 스위치 탭을 선택합니다.
23. Add standard virtual 스위치를 선택합니다.
24. vSwitch Name에 대한 iSciSciBootvSwitch-B의 이름을 입력합니다.
25. MTU를 9000으로 설정합니다.
26. 업링크 1 드롭다운 메뉴에서 vmnic3 을 선택합니다.
27. 추가 를 클릭합니다.
28. 가운데 창에서 VMkernel NIC 탭을 선택합니다.
29. Add VMkernel NIC 를 선택합니다
30. iSciBootPG-B의 새 포트 그룹 이름을 지정합니다
31. 가상 스위치용 iSciSciBootvSwitch-B를 선택합니다.
32. MTU를 9000으로 설정합니다. VLAN ID를 입력하지 마십시오.
33. IPv4 설정에 대해 정적 을 선택하고 옵션을 확장하여 구성 내에서 주소 및 서브넷 마스크를 제공합니다.

IP 주소 충돌을 피하기 위해 Cisco UCS iSCSI IP 풀 주소를 재할당해야 하는 경우 iSCSI VMkernel 포트에 대해 동일한 서브넷에 있는 다른 IP 주소를 사용하는 것이 좋습니다.

34. 생성 을 클릭합니다.
35. 왼쪽에서 네트워킹 을 선택한 다음 포트 그룹 탭을 선택합니다.
36. 가운데 창에서 VM Network를 마우스 오른쪽 버튼으로 클릭하고 Remove를 선택합니다.
37. 제거를 클릭하여 포트 그룹 제거를 완료합니다.
38. 가운데 창에서 포트 그룹 추가를 선택합니다.
39. 포트 그룹 관리 네트워크의 이름을 지정하고 VLAN ID 필드에 '<IB-mgmt-vlan-id>'를 입력한 다음 가상 스위치 vSwitch0이 선택되어 있는지 확인합니다.
40. 추가 를 클릭하여 IB-MGMT Network에 대한 편집을 마칩니다.
41. 맨 위에서 VMkernel NIC 탭을 선택합니다.
42. Add VMkernel NIC를 클릭합니다.
43. 새 포트 그룹의 경우 VMotion을 입력합니다.
44. 가상 스위치의 경우 vSwitch0 선택됨 을 선택합니다.
45. VLAN ID에 '<vMotion-vlan-id>'를 입력합니다.
46. MTU를 9000으로 변경합니다.
47. 정적 IPv4 설정을 선택하고 IPv4 설정을 확장합니다.
48. ESXi 호스트 vMotion IP 주소와 넷마스크를 입력합니다.
49. vMotion 스택 TCP/IP 스택을 선택합니다.
50. Services 아래에서 vMotion을 선택합니다.
51. 생성 을 클릭합니다.
52. Add VMkernel NIC를 클릭합니다.
53. 새 포트 그룹에 NFS_Share를 입력합니다.
54. 가상 스위치의 경우 vSwitch0 선택됨 을 선택합니다.
55. VLAN ID에 '<infra-nfs-vlan-id>'를 입력합니다
56. MTU를 9000으로 변경합니다.
57. 정적 IPv4 설정을 선택하고 IPv4 설정을 확장합니다.
58. ESXi 호스트 인프라스트럭처 NFS IP 주소와 넷마스크를 입력합니다.
59. 서비스를 선택하지 마십시오.
60. 생성 을 클릭합니다.
61. 가상 스위치 탭을 선택한 다음 vSwitch0을 선택합니다. vSwitch0 VMkernel NIC의 속성은 다음 예와 유사해야 합니다.



62. VMkernel NIC 탭을 선택하여 구성된 가상 어댑터를 확인합니다. 나열된 어댑터는 다음 예와 비슷해야 합니다.



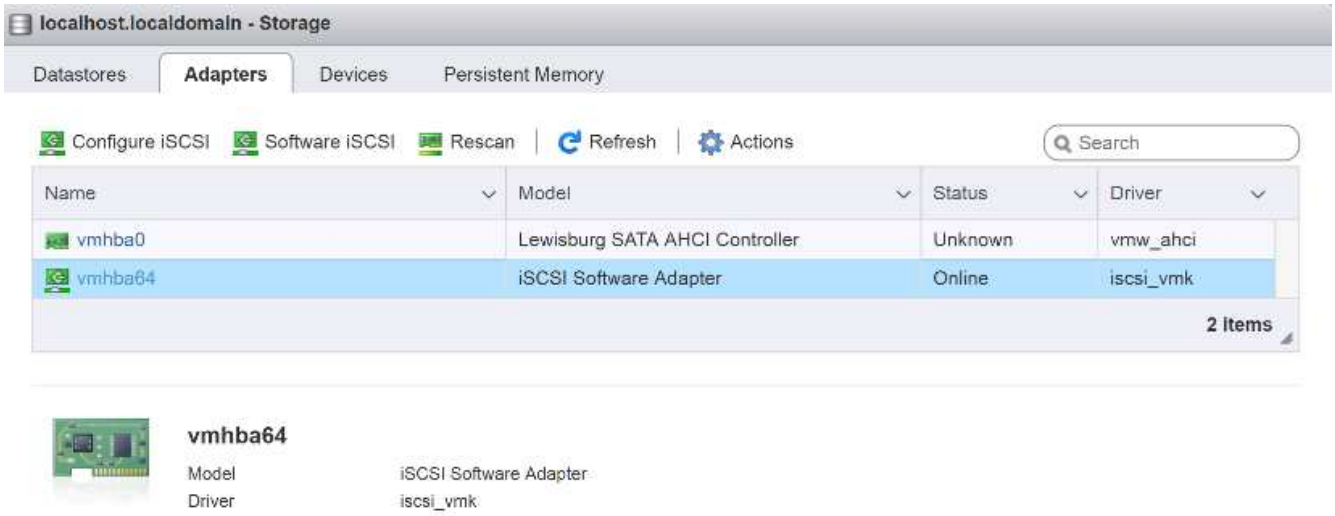
iSCSI 다중 경로를 설정합니다

ESXi 호스트 VM-Host-Infra-01 및 VM-Host-Infra-02

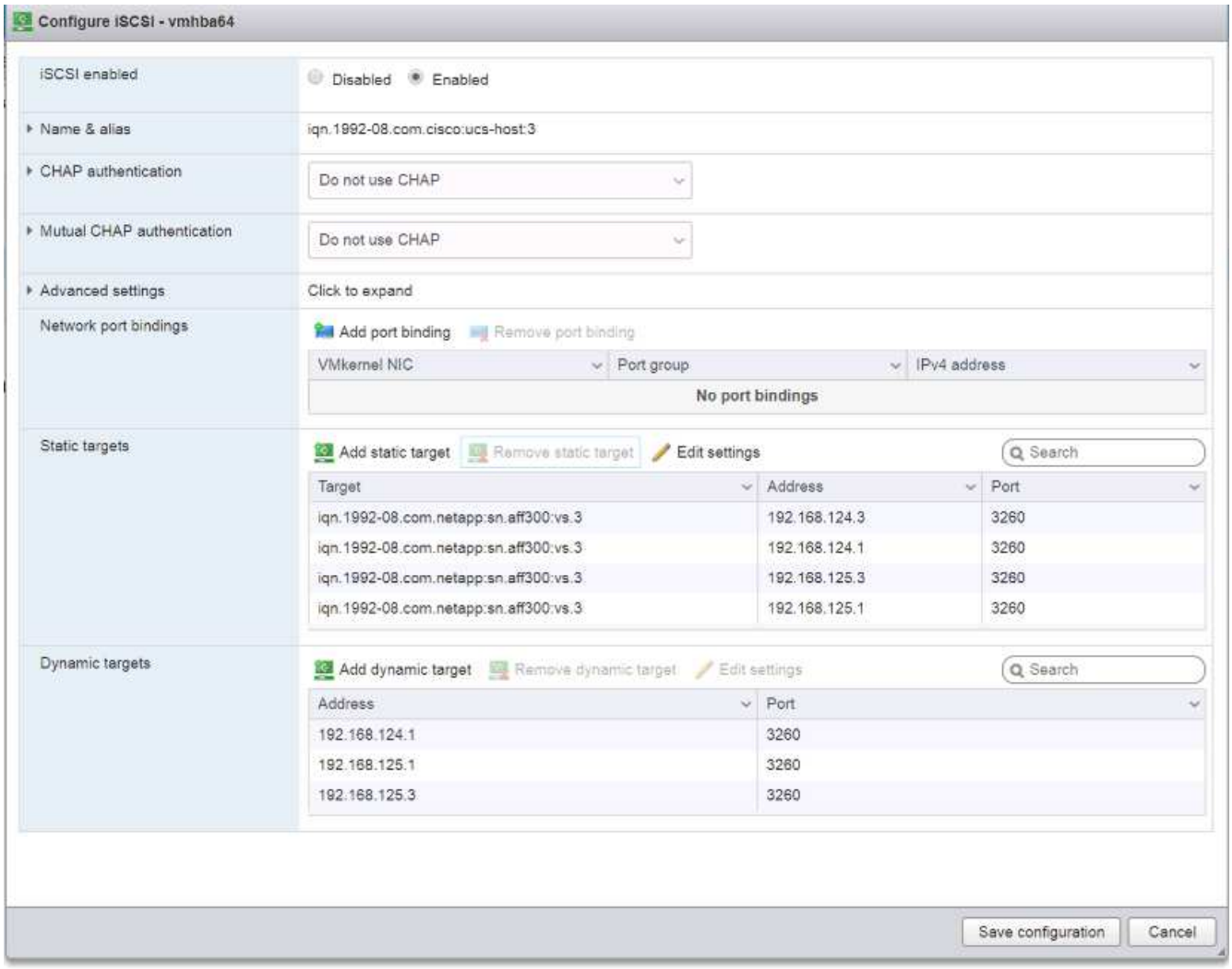
ESXi 호스트에서 iSCSI 다중 경로를 설정하려면 VM-Host-Infra-01 및 VM-Host-Infra-02를 수행하고 다음 단계를 수행하십시오.

1. 각 호스트 클라이언트에서 왼쪽의 Storage 를 선택합니다.

2. 가운데 창에서 어댑터를 클릭합니다.
3. iSCSI 소프트웨어 어댑터를 선택하고 iSCSI 구성 을 클릭합니다.



4. 동적 대상 아래에서 동적 대상 추가를 클릭합니다.
5. ISCSI_liff 01a IP Address를 입력한다.
6. iSCSI_liff 01b, iSCSI_liff 02a, iSCSI_liff 02b 등의 IP 주소를 다시 입력합니다.
7. 구성 저장 을 클릭합니다.



모든 "iscsi_lif" IP 주소를 얻으려면 NetApp 스토리지 클러스터 관리 인터페이스에 로그인하고 "network interface show" 명령을 실행하십시오.

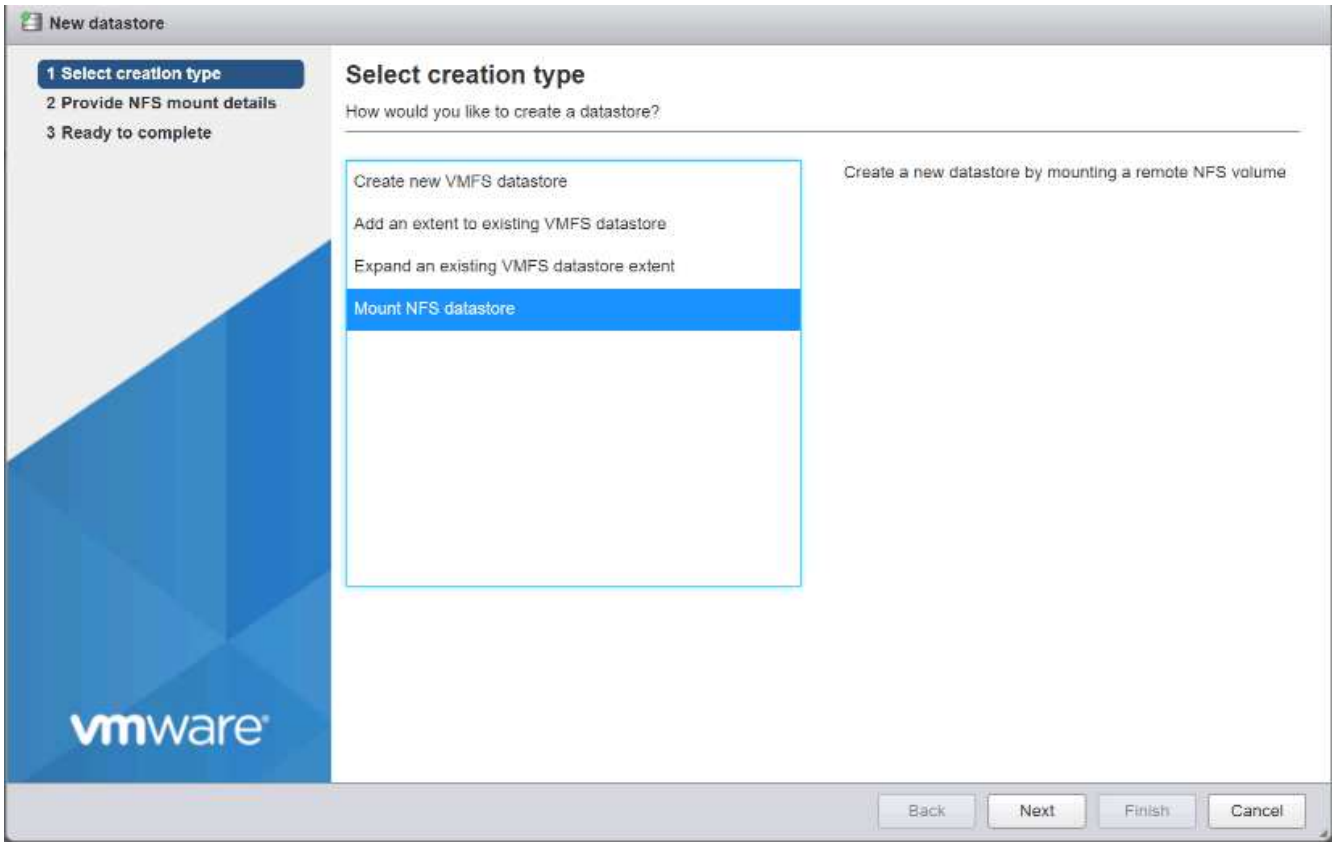
호스트가 스토리지 어댑터를 자동으로 다시 검사하며 대상은 정적 대상에 추가됩니다.

필수 데이터 저장소를 마운트합니다

ESXi 호스트 VM-Host-Infra-01 및 VM-Host-Infra-02

필요한 데이터 저장소를 마운트하려면 각 ESXi 호스트에서 다음 단계를 수행합니다.

1. 호스트 클라이언트 에서 왼쪽에 있는 스토리지 를 선택합니다.
2. 가운데 창에서 데이터 저장소 를 선택합니다.
3. 가운데 창에서 새 데이터 저장소 를 선택하여 새 데이터 저장소를 추가합니다.
4. 새 데이터 저장소 대화 상자에서 NFS 데이터 저장소 마운트 를 선택하고 다음 을 클릭합니다.

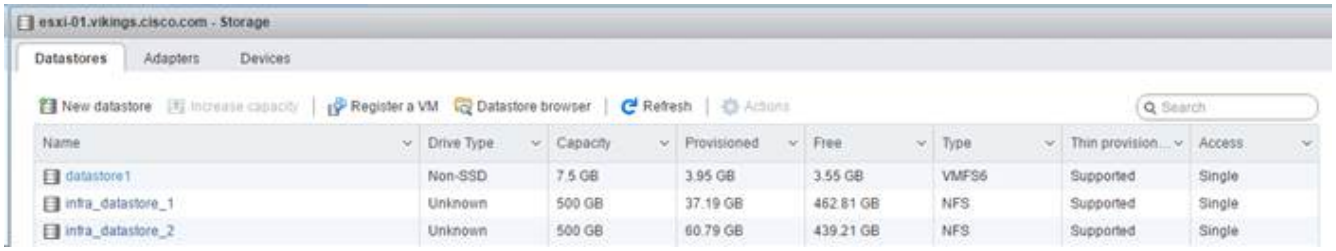


5. NFS 마운트 세부 정보 제공 페이지에서 다음 단계를 완료합니다.
   a. 데이터 저장소 이름에 'infra_datastore_1'을 입력합니다.
   b. NFS 서버에 대한 NFS_liff 01_a LIF의 IP 주소를 입력합니다.
   c. NFS 공유에 대해 '/infra_datastore_1'을 입력합니다.
   d. NFS 버전은 NFS 3으로 설정된 상태로 둡니다.
   e. 다음 을 클릭합니다.

6. 마침 을 클릭합니다. 이제 데이터 저장소가 데이터 저장소 목록에 표시됩니다.
7. 가운데 창에서 새 데이터 저장소 를 선택하여 새 데이터 저장소를 추가합니다.
8. New Datastore 대화 상자에서 Mount NFS Datastore를 선택하고 Next를 클릭합니다.
9. NFS 마운트 세부 정보 제공 페이지에서 다음 단계를 완료합니다.

a. 데이터 저장소 이름에 infra_datastore_2 를 입력합니다.
b. NFS 서버에 대한 NFS_liff 02_a LIF의 IP 주소를 입력합니다.
c. NFS 공유에 대해 '/infra_datastore_2'를 입력합니다.
d. NFS 버전은 NFS 3으로 설정된 상태로 둡니다.
e. 다음 을 클릭합니다.

10. 마침 을 클릭합니다. 이제 데이터 저장소가 데이터 저장소 목록에 표시됩니다.



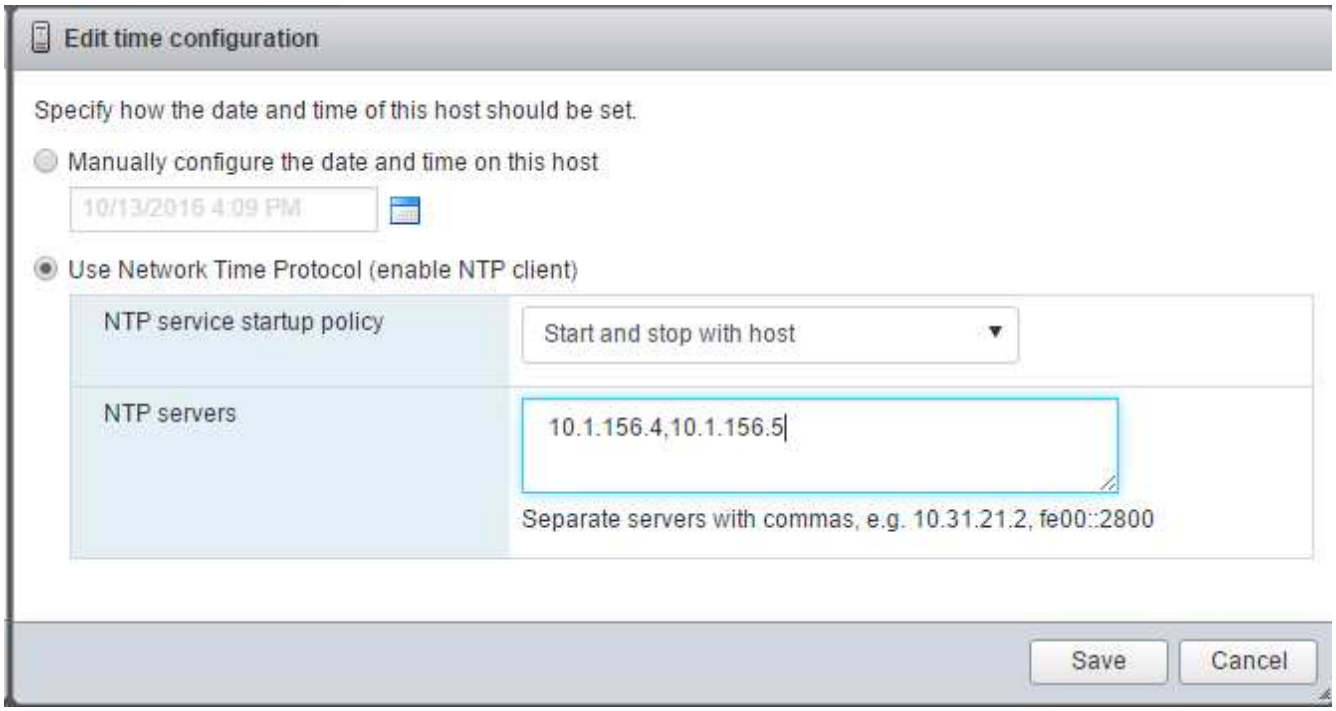
11. 두 ESXi 호스트에 두 데이터 저장소를 모두 마운트합니다.

ESXi 호스트에서 **NTP**를 구성합니다

ESXi 호스트 VM-Host-Infra-01 및 VM-Host-Infra-02

ESXi 호스트에서 NTP를 구성하려면 각 호스트에서 다음 단계를 수행합니다.

1. Host Client의 왼쪽에 있는 Manage를 선택합니다.
2. 가운데 창에서 시간 및 날짜 탭을 선택합니다.
3. 설정 편집 을 클릭합니다.
4. Use Network Time Protocol (enable NTP client)(네트워크 시간 프로토콜 사용(NTP 클라이언트 활성화)) 이 선택되어 있는지 확인합니다.
5. 드롭다운 메뉴를 사용하여 Start and Stop with Host 를 선택합니다.
6. NTP 서버 상자에 두 개의 Nexus 스위치 NTP 주소를 쉼표로 구분하여 입력합니다.



7. 저장 을 클릭하여 구성 변경 사항을 저장합니다.
8. Actions > NTP Service > Start 를 선택합니다.
9. 이제 NTP 서비스가 실행되고 있으며 시계가 대략 올바른 시간으로 설정되어 있는지 확인합니다

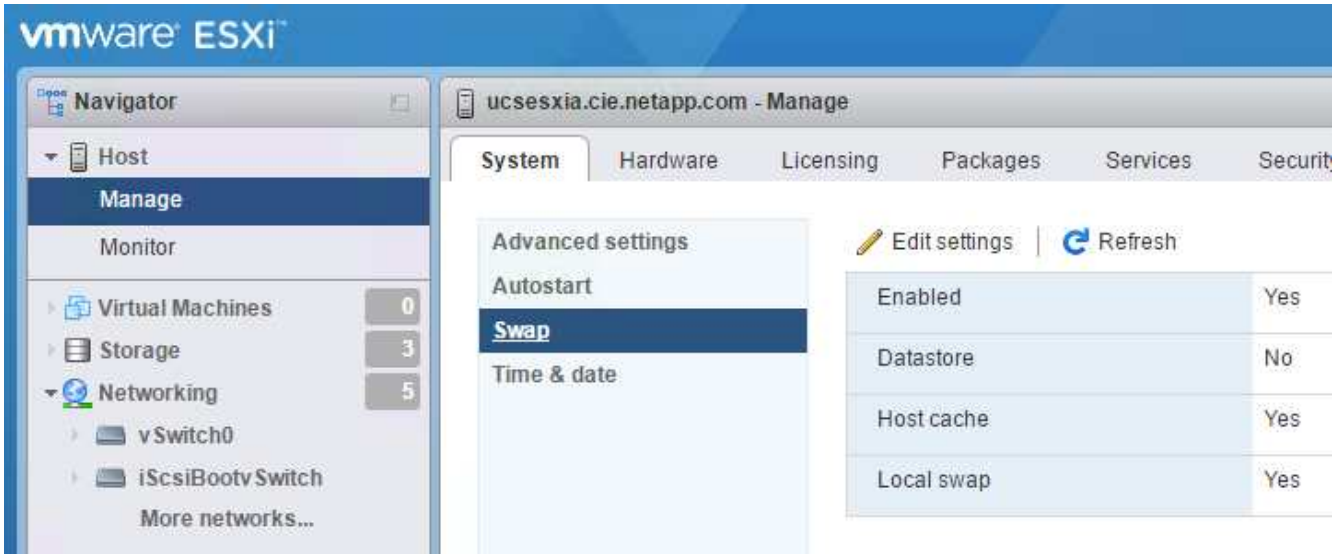
NTP 서버 시간은 호스트 시간과 약간 다를 수 있습니다.

ESXi 호스트 스왑을 구성합니다

ESXi 호스트 VM-Host-Infra-01 및 VM-Host-Infra-02

ESXi 호스트에서 호스트 스왑을 구성하려면 각 호스트에서 다음 단계를 수행합니다.

1. 왼쪽 탐색 창에서 관리 를 클릭합니다. 오른쪽 창에서 System을 선택하고 Swap을 클릭합니다.



2. 설정 편집 을 클릭합니다. Datastore 옵션에서 infra_swap을 선택합니다.

3. 저장 을 클릭합니다.

VMware VAAI용 NetApp NFS 플러그인 1.1.2를 설치합니다

NetApp NFS 플러그인 1을 설치합니다. 1.2 VMware VAAI의 경우 다음 단계를 완료합니다.

1. NetApp NFS Plug-in for VMware VAAI 다운로드:
   a. 로 이동합니다 "NetApp 소프트웨어 다운로드 페이지".
   b. 아래로 스크롤하여 VMware VAAI용 NetApp NFS 플러그인 을 클릭합니다.
   c. ESXi 플랫폼을 선택합니다.
   d. 최신 플러그인의 오프라인 번들(.zip) 또는 온라인 번들(.vib)을 다운로드합니다.
2. VMware VAAI용 NetApp NFS 플러그인은 ONTAP 9.5에서 IMT 자격 평가를 보류 중이며, 상호 운용성 세부 정보가 곧 NetApp IMT에 게시될 예정입니다.
3. ESX CLI를 사용하여 ESXi 호스트에 플러그인을 설치합니다.
4. ESXi 호스트를 재부팅합니다.

VMware vCenter Server 6.7을 설치합니다

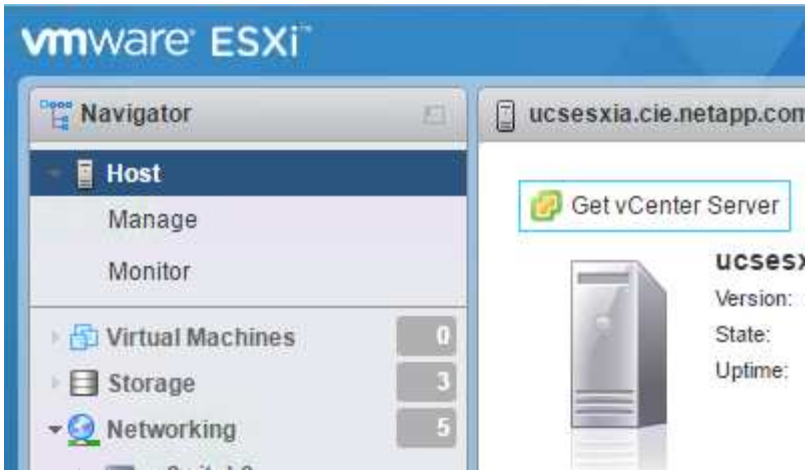
이 섹션에서는 FlexPod Express 구성에 VMware vCenter Server 6.7을 설치하는 절차를 자세히 설명합니다.

FlexPod Express는 VCSA(VMware vCenter Server Appliance)를 사용합니다.

VMware vCenter Server 어플라이언스를 설치합니다

VCSA를 설치하려면 다음 단계를 완료하십시오.

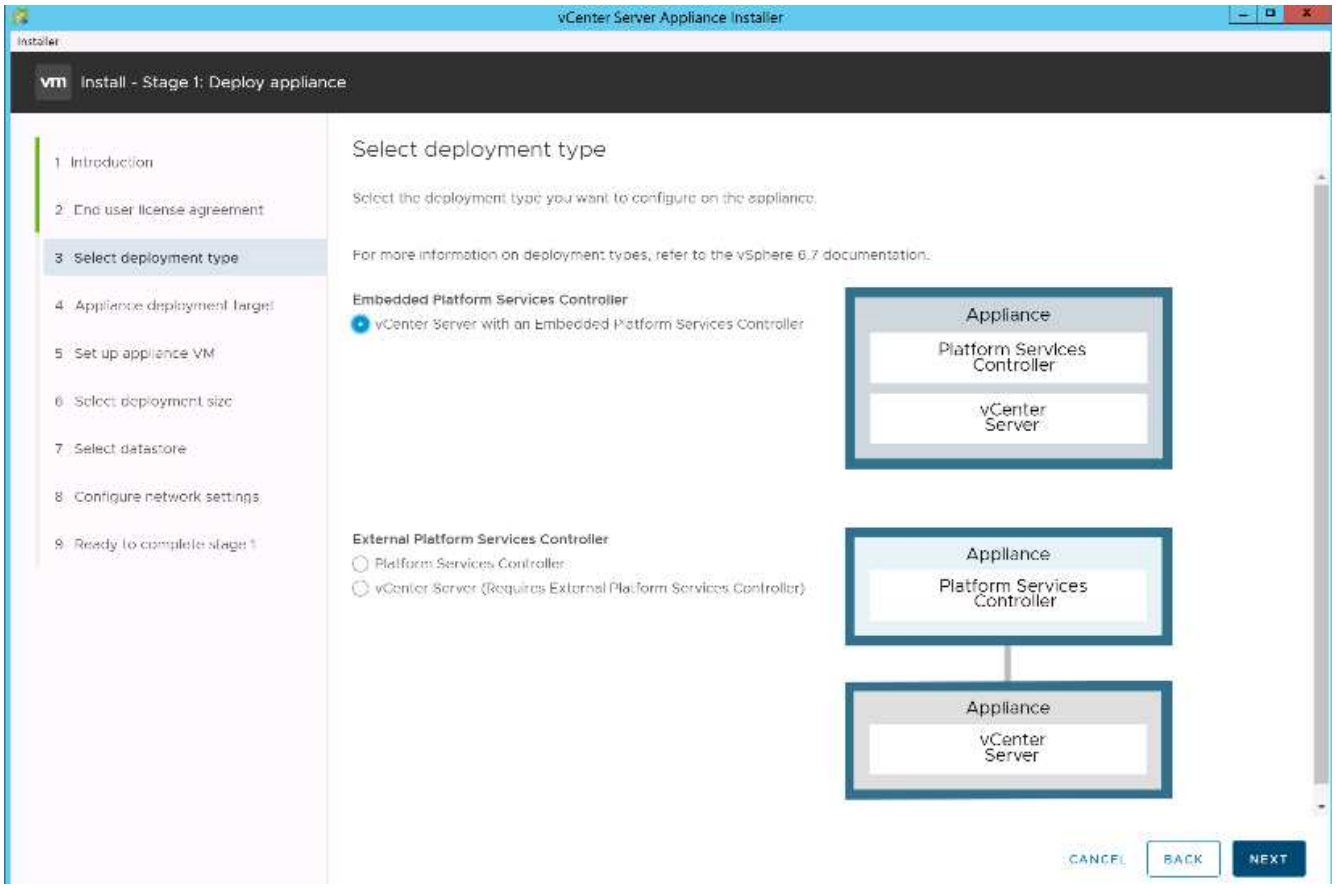
1. VCSA를 다운로드합니다. ESXi 호스트를 관리할 때 vCenter Server 가져오기 아이콘을 클릭하여 다운로드 링크를 액세스합니다.



2. VMware 사이트에서 VCSA를 다운로드합니다.

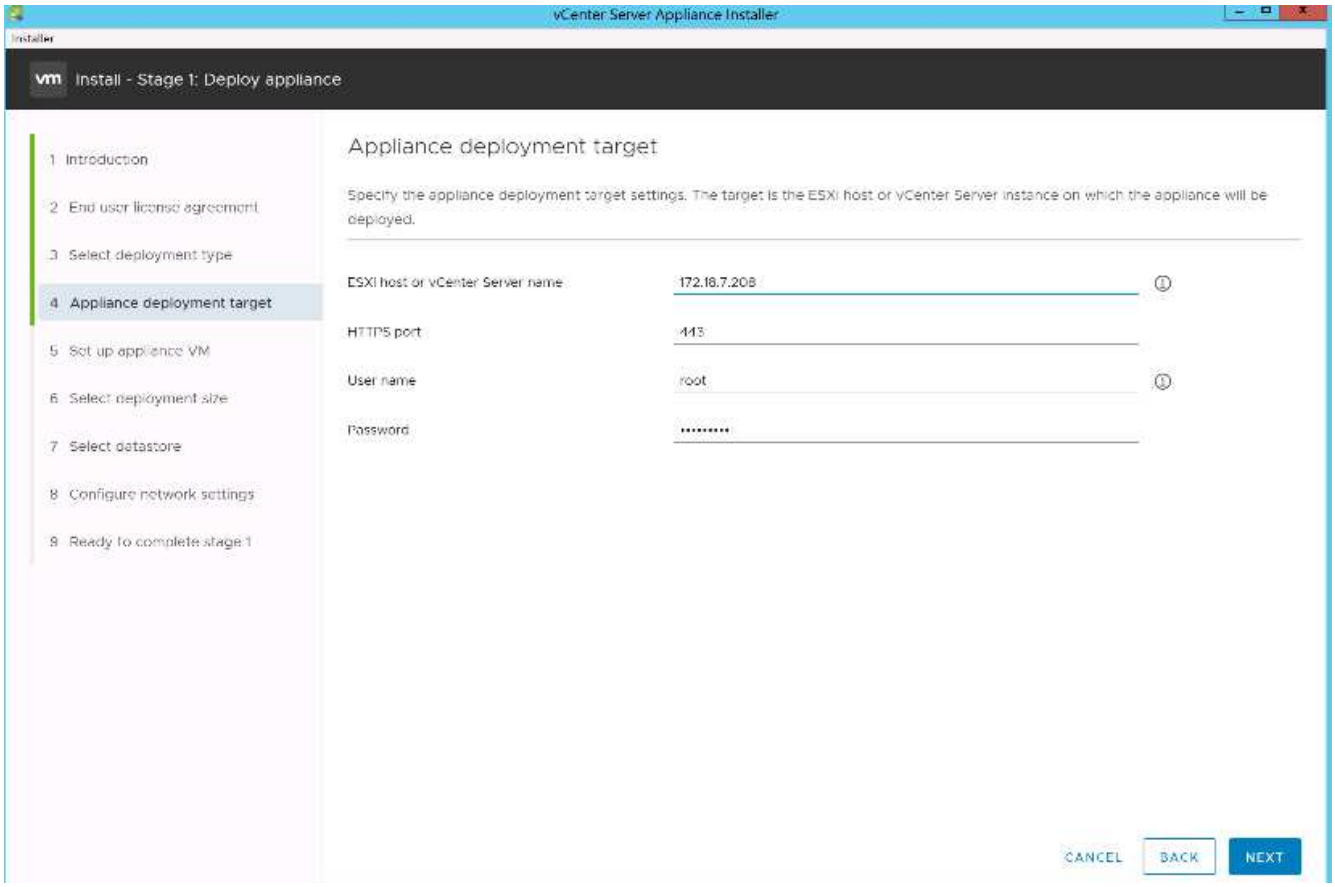
> Microsoft Windows vCenter Server 설치 가능한 가 지원되지만 VMware는 새로운 구축에 VCSA를 권장합니다.

3. ISO 이미지를 마운트합니다.
4. vcsa-UI-installer>'Win32' 디렉토리로 이동합니다. installer.exe를 두 번 클릭합니다.
5. 설치 를 클릭합니다.
6. 소개 페이지에서 다음 을 클릭합니다.
7. EULA에 동의합니다.
8. 배포 유형으로 임베디드 플랫폼 서비스 컨트롤러 를 선택합니다.

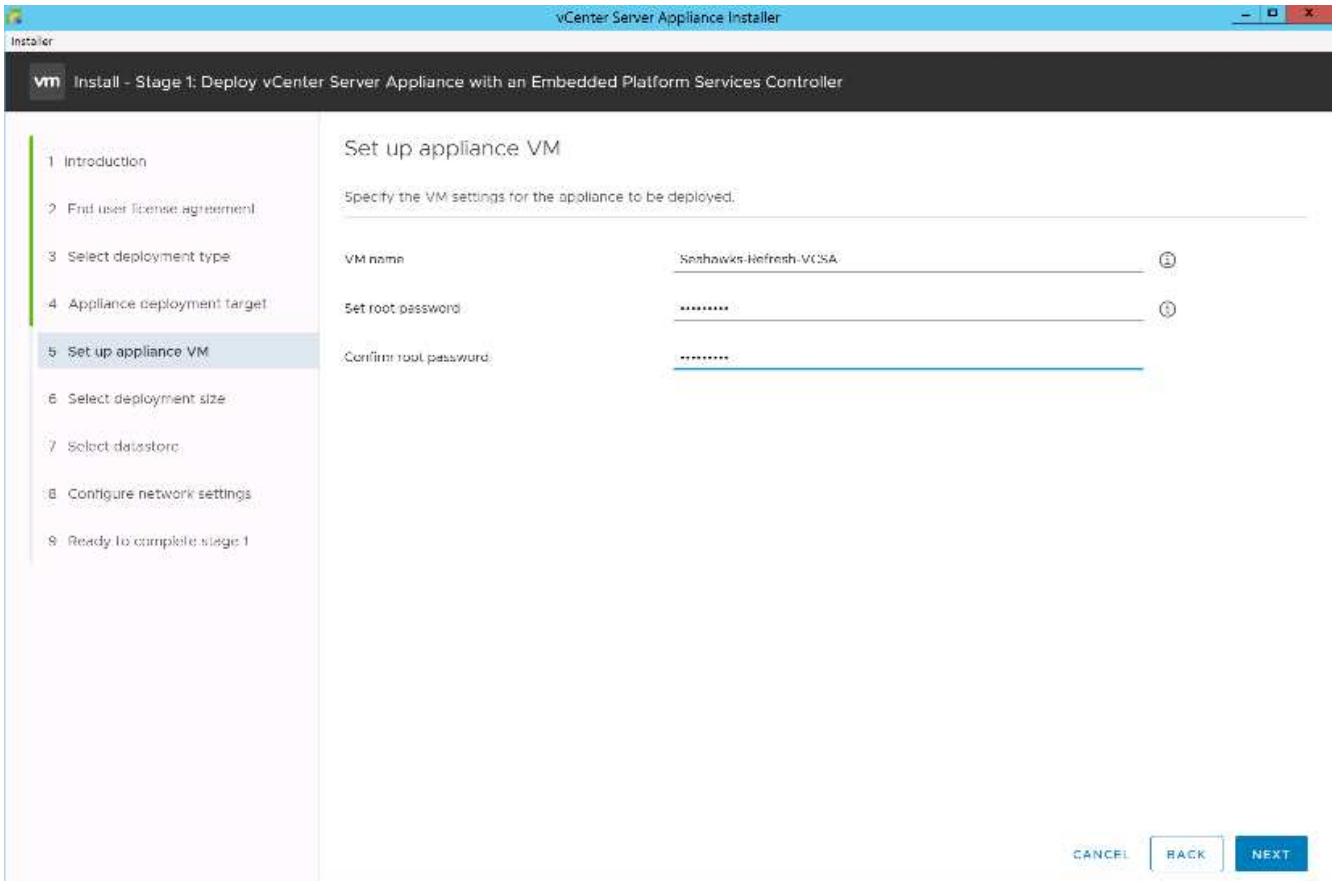


필요한 경우 외부 플랫폼 서비스 컨트롤러 배포도 FlexPod Express 솔루션의 일부로 지원됩니다.

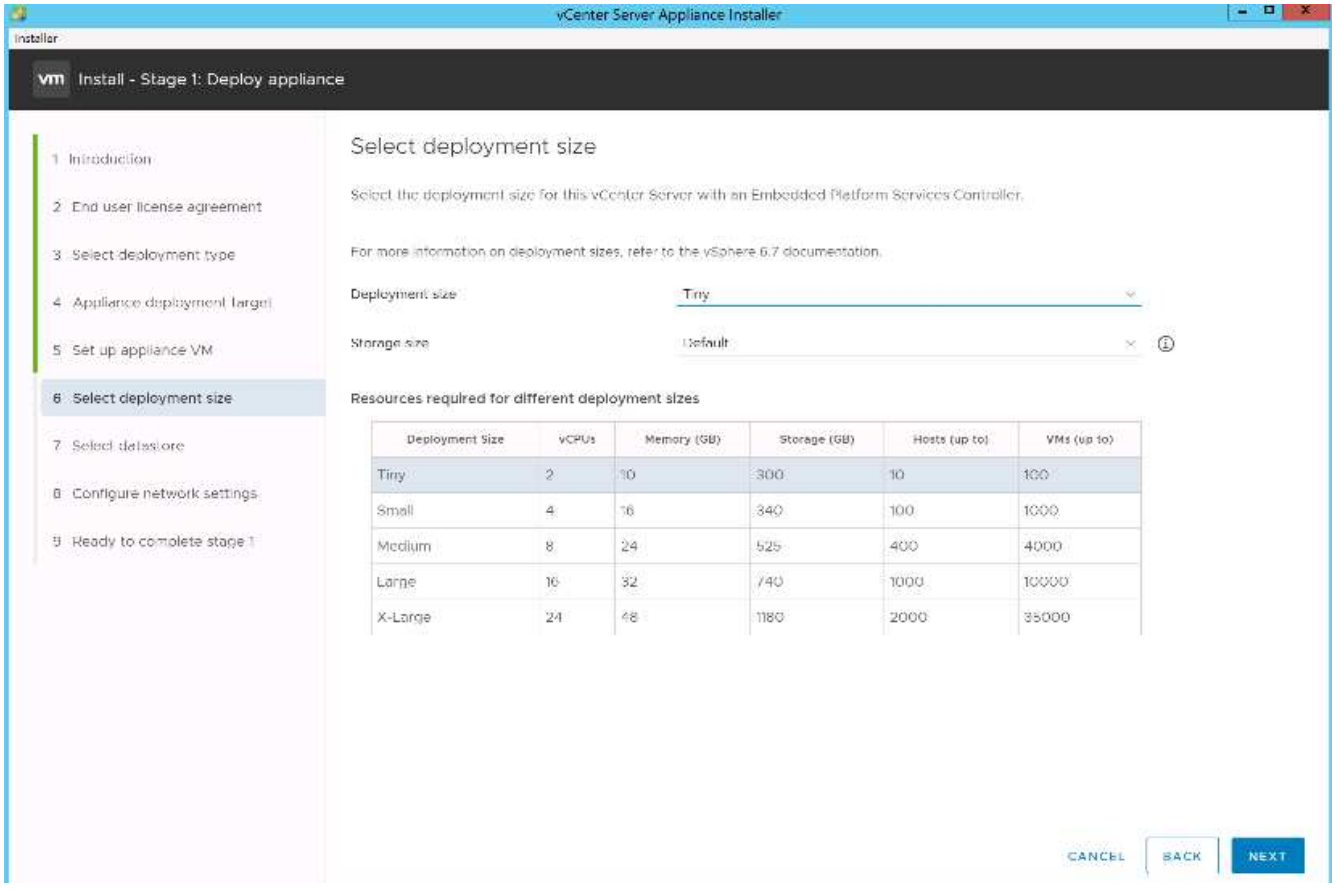
9. 어플라이언스 배포 대상 페이지에서 배포한 ESXi 호스트의 IP 주소, 루트 사용자 이름 및 루트 암호를 입력합니다. 다음 을 클릭합니다.



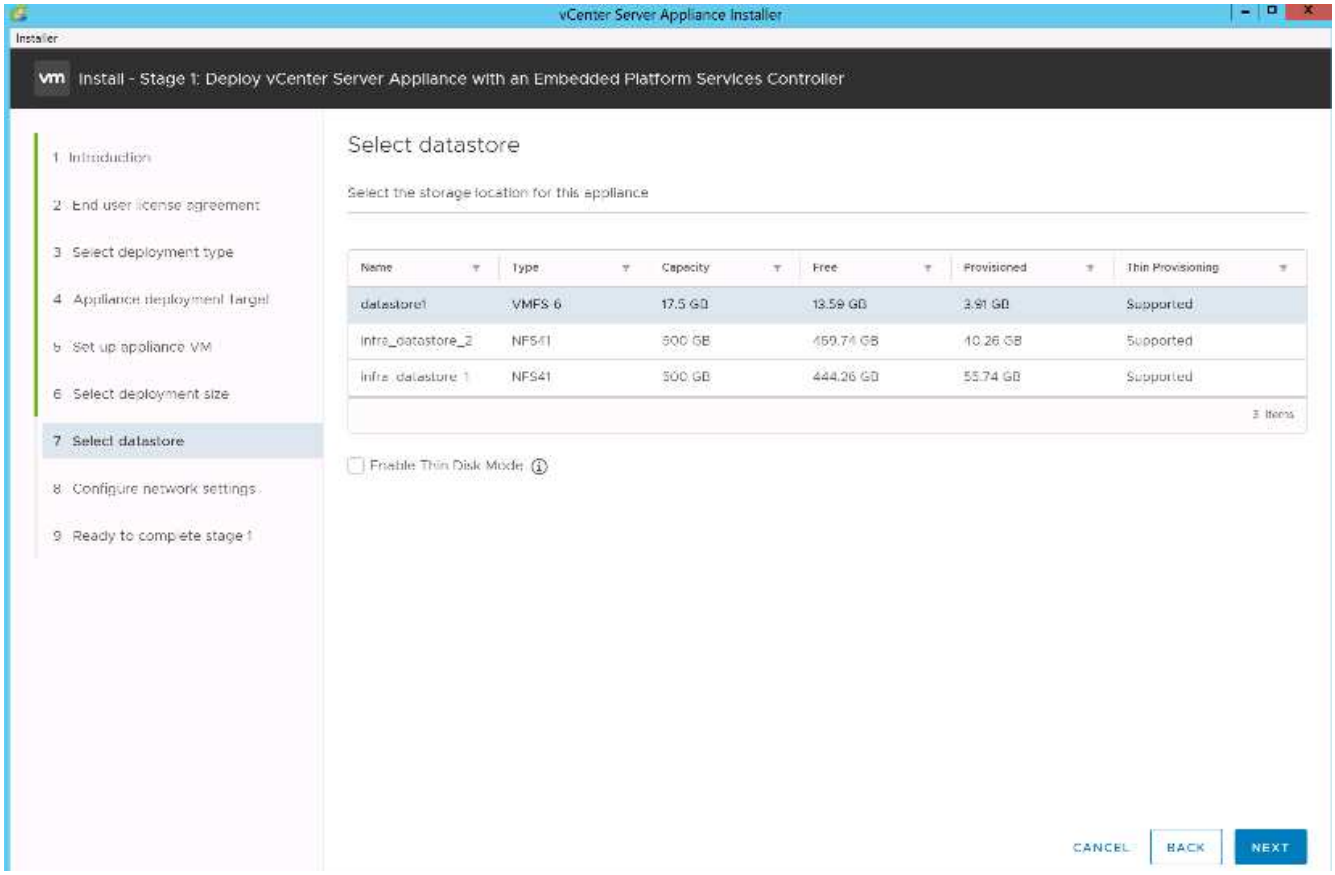
10. VCSA를 VM 이름으로 입력하고 VCSA에 사용할 루트 암호를 입력하여 어플라이언스 VM을 설정합니다. 다음 을 클릭합니다.



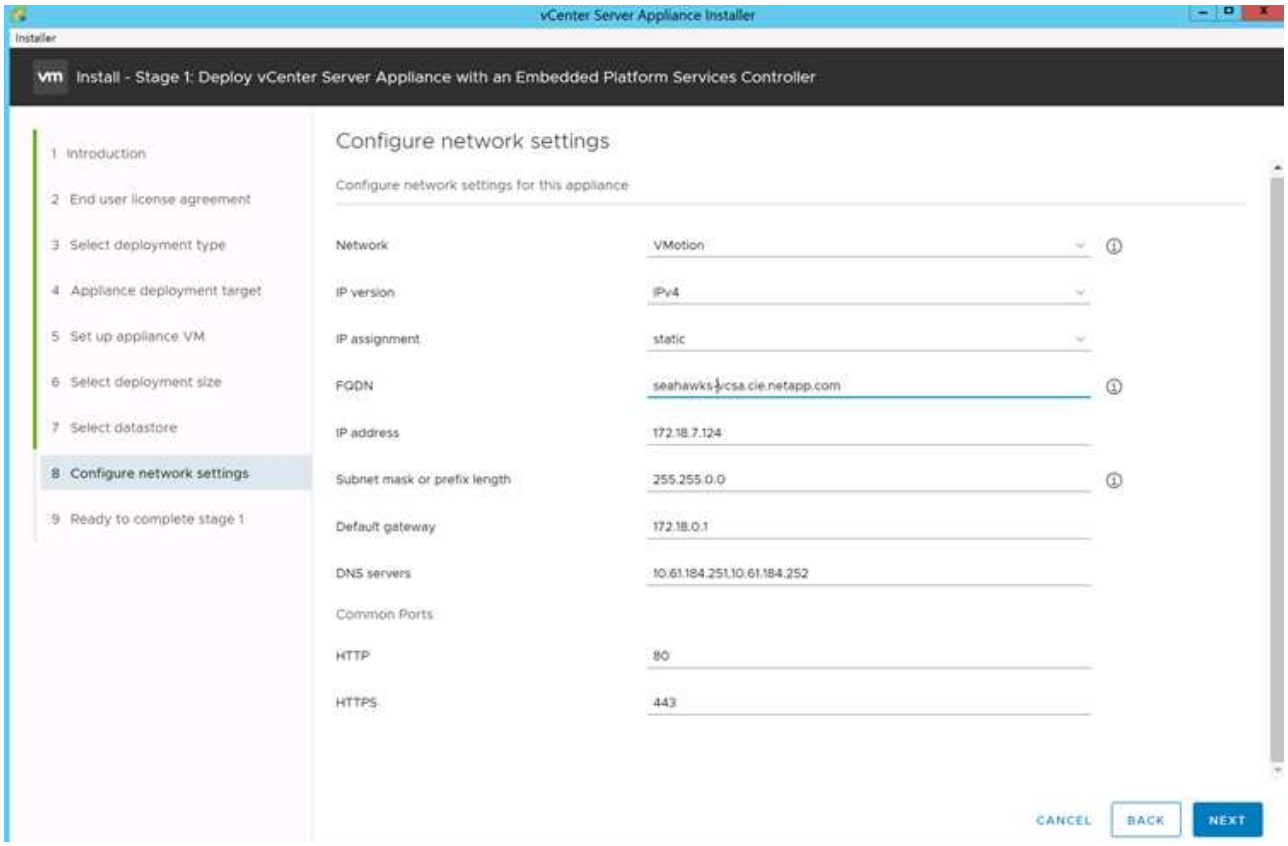
11. 환경에 가장 적합한 구축 크기를 선택합니다. 다음 을 클릭합니다.



12. 'infra_datastore_1' 데이터 저장소를 선택합니다. 다음 을 클릭합니다.



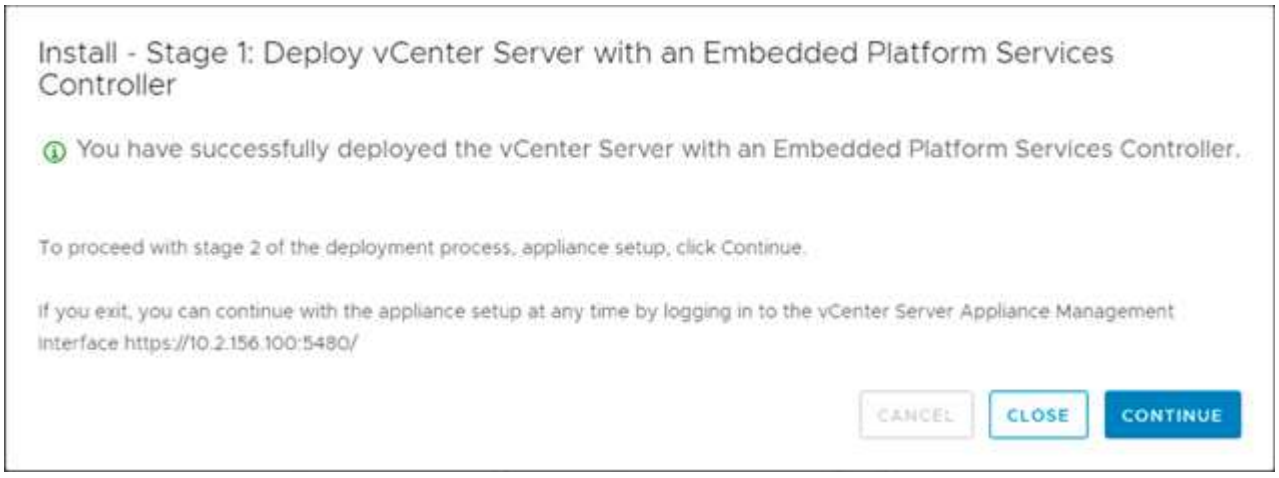
13. 네트워크 설정 구성 페이지에서 다음 정보를 입력하고 다음 을 클릭합니다.
    a. MGMT-Network를 네트워크로 선택합니다.
    b. VCSA에 사용할 FQDN 또는 IP를 입력합니다.
    c. 사용할 IP 주소를 입력합니다.
    d. 사용할 서브넷 마스크를 입력합니다.
    e. 기본 게이트웨이를 입력합니다.
    f. DNS 서버를 입력합니다.



14. 1단계 완료 준비 페이지에서 입력한 설정이 올바른지 확인합니다. 마침 을 클릭합니다.

    VCSA가 지금 설치됩니다. 이 과정은 몇 분 정도 소요됩니다.

15. 1단계가 완료되면 완료되었다는 메시지가 나타납니다. 계속 을 클릭하여 2단계 구성을 시작합니다.



16. 2단계 소개 페이지에서 다음 을 클릭합니다.
17. NTP 서버 주소에 대해 '<<var_ntp_id>>'를 입력합니다. 여러 NTP IP 주소를 입력할 수 있습니다.

    vCenter Server 고가용성을 사용하려는 경우 SSH 액세스가 설정되어 있는지 확인합니다.

18. SSO 도메인 이름, 암호 및 사이트 이름을 구성합니다. 다음 을 클릭합니다.

특히 "vsphere.local" 도메인 이름을 벗어나는 경우 이러한 값을 참조로 기록합니다.

19. 원하는 경우 VMware 고객 경험 프로그램에 참여하십시오. 다음 을 클릭합니다.
20. 설정 요약을 봅니다. 마침 을 클릭하거나 뒤로 단추를 사용하여 설정을 편집합니다.
21. 설치가 시작된 후 설치를 일시 중지하거나 중지할 수 없다는 메시지가 나타납니다. 계속하려면 확인을 클릭하십시오.

    어플라이언스 설정이 계속됩니다. 이 작업은 몇 분 정도 걸립니다.

    설정이 성공했음을 나타내는 메시지가 나타납니다.

    vCenter Server에 액세스하기 위해 설치 관리자가 제공하는 링크를 클릭할 수 있습니다.

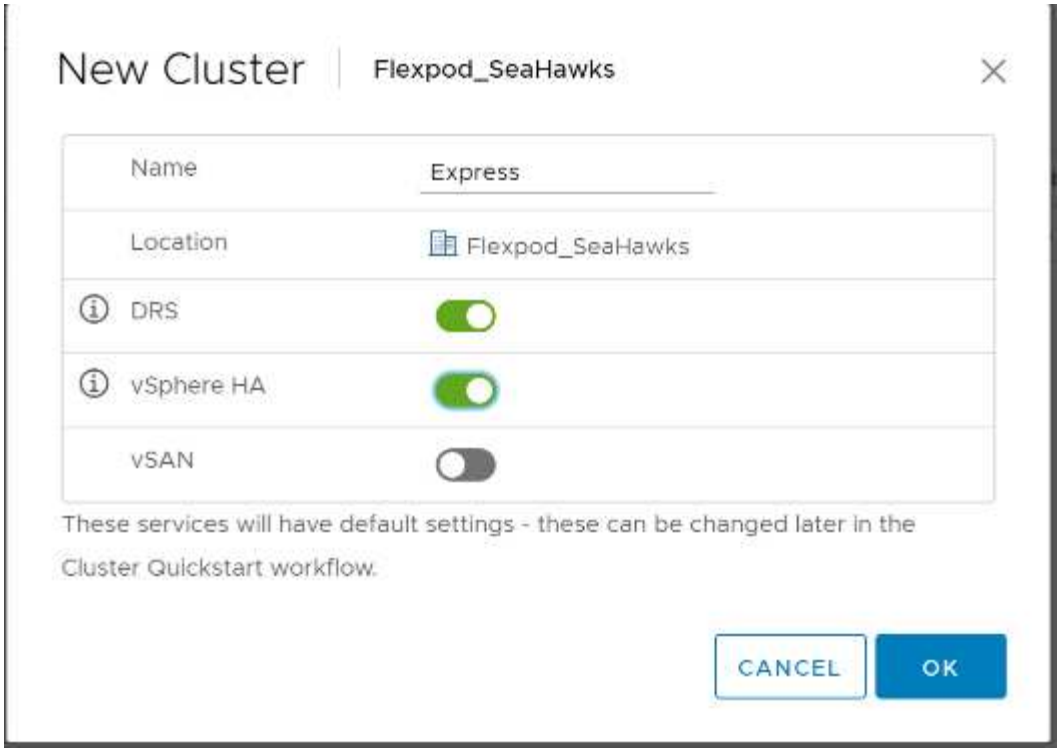
VMware vCenter Server 6.7 및 **vSphere** 클러스터링 구성

VMware vCenter Server 6.7 및 vSphere 클러스터링을 구성하려면 다음 단계를 수행하십시오.

1. https://\<<FQDN 또는 vCenter의 IP >>/vSphere-client/로 이동합니다.
2. vSphere Client 시작 을 클릭합니다.
3. 사용자 이름 administrator@vsphere.loca l 과 VCSA 설정 프로세스 중에 입력한 SSO 암호를 사용하여 로그인합니다.
4. vCenter 이름을 마우스 오른쪽 버튼으로 클릭하고 New Datacenter를 선택합니다.
5. 데이터 센터의 이름을 입력하고 확인 을 클릭합니다.
    - vSphere 클러스터를 생성합니다. *

vSphere 클러스터를 생성하려면 다음 단계를 수행하십시오.

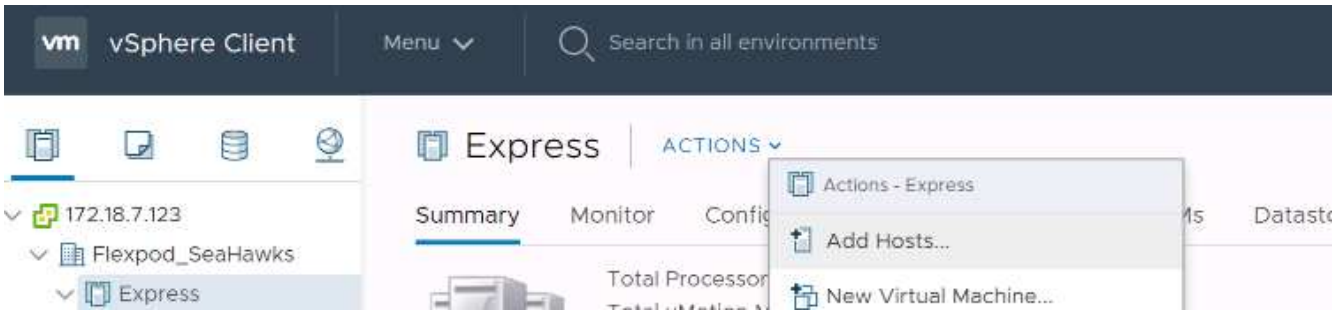
1. 새로 생성된 데이터 센터를 마우스 오른쪽 버튼으로 클릭하고 New Cluster를 선택합니다.
2. 클러스터의 이름을 입력합니다.
3. DRS 및 vSphere HA 옵션을 선택하고 설정합니다.
4. 확인 을 클릭합니다.



◦ 클러스터에 ESXi 호스트 추가 *

클러스터에 ESXi 호스트를 추가하려면 다음 단계를 수행하십시오.

1. 클러스터의 Actions 메뉴에서 Add Host를 선택합니다.



2. 클러스터에 ESXi 호스트를 추가하려면 다음 단계를 수행하십시오.
   a. 호스트의 IP 또는 FQDN을 입력합니다. 다음 을 클릭합니다.
   b. 루트 사용자 이름과 암호를 입력합니다. 다음 을 클릭합니다.
   c. 예를 클릭하여 호스트의 인증서를 VMware 인증서 서버에서 서명한 인증서로 바꿉니다.
   d. 호스트 요약 페이지에서 다음 을 클릭합니다.
   e. 녹색 + 아이콘을 클릭하여 vSphere 호스트에 라이센스를 추가합니다.

      이 단계는 원할 경우 나중에 완료할 수 있습니다.

   f. 다음 을 클릭하여 잠금 모드를 해제합니다.
   g. VM 위치 페이지에서 다음 을 클릭합니다.

h. 완료 준비 페이지를 검토합니다. 뒤로 단추를 사용하여 변경하거나 마침 을 선택합니다.

3. Cisco UCS 호스트 B에 대해 1단계와 2단계를 반복합니다

FlexPod Express 구성에 추가된 모든 호스트에 대해 이 프로세스를 완료해야 합니다.

ESXi 호스트에서 코어 덤프를 구성합니다

iSCSI 부팅 호스트에 대한 ESXi Dump Collector 설정

VMware iSCSI 소프트웨어 이니시에이터를 사용하여 iSCSI로 부팅된 ESXi 호스트는 vCenter의 일부인 ESXi 덤프 수집기로 코어 덤프를 수행하도록 구성해야 합니다. 덤프 수집기는 vCenter 어플라이언스에서 기본적으로 사용되지 않습니다. 이 절차는 vCenter 구축 섹션의 마지막에 실행해야 합니다. ESXi 덤프 수집기를 설정하려면 다음 단계를 수행하십시오.

1. vSphere Web Client에 mailto:administrator@vsphere.loca l[administrator@vsphere.loca l^]으로 로그인하고 Home을 선택합니다.
2. 가운데 창에서 시스템 구성 을 클릭합니다.
3. 왼쪽 창에서 서비스를 선택합니다.
4. 서비스 에서 VMware vSphere ESXi Dump Collector 를 클릭합니다.
5. 중앙 창에서 녹색 시작 아이콘을 클릭하여 서비스를 시작합니다.
6. 작업 메뉴에서 시작 유형 편집을 클릭합니다.
7. 자동을 선택합니다.
8. 확인 을 클릭합니다.
9. SSH를 루트로 사용하여 각 ESXi 호스트에 연결합니다.
10. 다음 명령을 실행합니다.

```
esxcli system coredump network set –v vmk0 –j <vcenter-ip>
esxcli system coredump network set –e true
esxcli system coredump network check
```

최종 명령어를 실행하면 Verified the configured netdump server is running 메시지가 나타난다.

FlexPod Express에 추가된 모든 호스트에 대해 이 프로세스를 완료해야 합니다.

결론

FlexPod Express는 업계 최고의 구성요소를 사용하는 검증된 설계를 통해 간단하고 효율적인 솔루션을 제공합니다. FlexPod Express는 추가 구성요소를 추가하여 특정 비즈니스 요구사항에 맞게 확장할 수 있습니다. FlexPod Express는 전용 솔루션이 필요한 중소기업, ROBO 및 기타 기업을 염두에 두고 설계되었습니다.

추가 정보

이 문서에 설명된 정보에 대해 자세히 알아보려면 다음 문서 및/또는 웹 사이트를 검토하십시오.

- NVA-1130-design:VMware vSphere 6.7U1 및 NetApp AFF A220을 포함하는 FlexPod Express with Direct-Attached IP = 기반 스토리지 NVA Design

  "https://www.netapp.com/us/media/nva-1130-design.pdf"

- AFF and FAS 시스템 설명서 센터 를 참조하십시오

  "http://docs.netapp.com/platstor/index.jsp"

- ONTAP 9 문서 센터

  "http://docs.netapp.com/ontap-9/index.jsp"

- NetApp 제품 설명서

  "https://docs.netapp.com"

FlexPod Express for VMware vSphere 7.0 with Cisco UCS Mini 및 NetApp AFF/FAS-NVA-Deployment

Jyh-shing Chen, NetApp

Cisco UCS Mini 및 NetApp AFF/FAS 솔루션이 포함된 VMware vSphere 7.0용 FlexPod Express는 B200 M5 블레이드 서버, Cisco UCS 6324 섀시 내 패브릭 인터커넥트, Cisco Nexus 31108PC-V 스위치 또는 기타 호환 스위치, NetApp AFF A220, C190 또는 FAS2700 시리즈 컨트롤러 HA 쌍을 지원하는 Cisco UCS Mini를 활용합니다. NetApp ONTAP 9.7 데이터 관리 소프트웨어를 실행합니다. 이 NVA(NetApp Verified Architecture) 구축 문서는 인프라 구성 요소를 구성하고 VMware vSphere 7.0 및 관련 툴을 구축하여 매우 안정적이고 가용성이 높은 FlexPod Express 기반 가상 인프라를 구축하는 데 필요한 세부 단계를 제공합니다.

"FlexPod Express for VMware vSphere 7.0 with Cisco UCS Mini 및 NetApp AFF/FAS-NVA-Deployment"